# Aff – Cyber 5G – BEJJ

#### What does this Affirmative say?

This affirmative argues that 5G networks are being rapidly deployed in a manner that lacks adequate cyber security standards. This risks hardware and software backdoors in 5G networks and equipment as nations purchase from and contract with untrusted vendors. The first advantage focusses on Commercial 5G and argues that NATO nations are at risk of cyber attacks on 5G networks that are unprecedented due to the degree of connectivity for basic functions and critical infrastructure that 5G will enable. The second scenario argues that NATO standardization would help Western nations counter Chinese 5G supremacy which is important in the tech race as 5G is a critical enabler of emerging and disruptive technology (many will run on/be dependent on 5G networks). The second advantage is about NATO military operations that will be conducted on 5G networks – most operations from data transfer to military communications will be conducted over 5G hardware because of benefits to range and speed. Many cards on both advantages have a ‘good 5G good, bad 5G bad’ angle that says 5G is inevitable, could solve many problems, or could introduce new and unprecedented security risks from IP theft and political coercion, to breaking military operations and communications.

#### Why is NATO key?

‘NATO key’ is pretty strong for this affirmative. The military advantage is about NATO so hard to solve that one without NATO – I suppose many teams are fiating we delete NATO and saying that’s good but the entire advantage is a defense of NATO and requires interoperability among NATO members. For the commercial 5G advantage, there’s a good argument that NATO cyber security experts best understand many of the security risks that 5G introduces for adopters. In truth the EU, ITU, or other telecommunications agencies could likely set standards for commercial technology and one weakness is that many of the 5G authors (even those advocating NATO action) argue that the EU is also important.

#### Why is security cooperation key?

Military integration requires DOD security standards given that the military will be reliant on 5G security networks.

#### Why is cyber key?

The internal links and solvency advocates are about cyber security of 5G networks---importantly the solvency mechanism and plan mandates are about cybersecurity standards only.

Thanks to Ahsan Tahirkheli, Ashrit Manduva, Avi Shah, Billy Blechman, Dani Roos, Iris Tsai, Ishaan Tipirneni, Katie Carpenter, Maggie Howerton, Raleigh Maxwell, and Sarah Kwon for their work on this file.

Feel free to email [gabjan@umich.edu](mailto:gabjan@umich.edu) with questions or concerns.

# 1AC

## 1AC

### Commercial 5G---1AC

#### Advantage 1 is Commercial 5G.

#### Current 5G deployment risks cyber backdoors in host nations---enables adversary blackmail, supply chain, and critical infrastructure attacks.

Giles ’22 [Keir; 7/4/2022; Senior Consulting Fellow at Chatham House, Director of the Conflict Studies Research Centre, Fellow at the National Security Center of Excellence Canada; Kim Hartmann; Cyber and Information Technology Director at the Conflict Studies Research Centre; "Emergence of 5G Networks and Implications for Cyber Conflict," https://doi.org/10.23919/CyCon55549.2022.9810903]

Western nations vary widely in their approach to the security of 5G networks and in the basic assumptions that drive their policy. This is clearly illustrated by the example of Huawei and other foreign technology providers being excluded from the development of 5G in some Western nations. While Sweden has excluded the two Chinese contributors, Huawei and ZTE, from participating in the development of 5G in Sweden (with Huawei filing an appeal against this ban),11 Norway has decided not to strictly ban the use of 5G equipment. Despite demands from the Norwegian government in December 2019, Telenor’s development of the 5G network in Bergen, Norway, is mostly based on Huawei sources and will remain so until 2024, when Telenor will remove untrusted sources due to security considerations.12 Austria initially decided not to rule out the use of Huawei technology in 5G networks but stated (under former chancellor Sebastian Kurz) that it would coordinate its actions with the EU.13 A more recent statement indicates that 5G may be built with Chinese contributions in Austria, serving Telekom Austria’s 25 million customers across Austria, Bulgaria, Croatia, Belarus, Slovenia, Serbia, and North Macedonia and using Chinese vendors in Bulgaria and North Macedonia for 4G.14 Belgium initially found no evidence of possible espionage through the utilization of Huawei’s technology and hence decided not to ban Huawei from contributions to the Belgian 5G network development.15 However, it was reported that Belgian operators Orange Belgium and Proximus dropped Huawei as a consequence of US pressure to exclude Chinese vendors.16 It was later reported that Belgium had previously experienced a pro-Huawei malign influence campaign.17 Britain decided to remove Huawei’s technology from its telecommunication networks and demanded its vendors reduce Huawei’s share of the network infrastructure to 35% by 2023.18 This process, which is expected to take until 2027, was instigated by the United States, alleging that Huawei posed a security threat due to its closeness to the Chinese government.19 Orange France decided to avoid using Chinese vendors when developing European 5G networks but envisions Huawei playing a role in the African 5G rollout.20 If there is a pattern among Western approaches to 5G security, it appears to be a consensus within the ‘Five Eyes’ partnership, and wide variance outside it.21

Many of the discussions around whether Huawei equipment (or software, as described above) should be used in 5G networks centred on the question of whether a ‘backdoor’ existed in available equipment. The crucial realization, however, is that the 5G architecture does not need ‘backdoors’ to be built into the system. The mere ability to contribute to the 5G core network constitutes a backdoor. The 5G architecture demands continuous integration and continuous deployment of function and software updates. As there is currently no valid option to automatically check code iterations for complex malicious execution options, this either must be monitored by IT professionals or will simply be based on trust in the contributor. The huge number of code iterations and updates that will propagate through a multitude of virtualizations makes it unlikely that this monitoring can be done by humans.

In addition, the complexity of the architecture and the distributed nature of its development opens up a still greater risk of supply chain attacks. In mid-2020, detection of the SolarWinds attack demonstrated the critical importance of software supply chain transparency and integrity (as well as the power of CI/CD attacks, as described above).22 It is equally vital that the construction of 5G network architecture for NATO member states is protected from hostile state interference – but this begs the question of how to exclude software providers owned by interests within those adversary states if they are already integrated into the network provision ecosystem.23

SECTION 3.

Strategic Goals of Adversaries In Networks of NATO Allies

It is essential that any new technology that introduces critical dependencies within NATO nations be adequately secured against threats from both non-state and state actors. This requires a full and regularly updated assessment of the aims and approaches to conflict of a wide range of possible adversaries. It also requires full and honest recognition of the threat among NATO allies themselves, and an acceptance that a state of notional peacetime does not mean that hostilities are not being waged by any available means.

The new vulnerabilities introduced by the specific nature of 5G networks lend themselves to a wide range of unfriendly and overtly hostile actions by adversaries. As with other forms of information threat, these span a broad spectrum of ambition, from simply causing damage with no other specific objective in mind, to high-level geostrategic change brought about through indirect means.24 Non-like-minded nations, including but not limited to Russia and China, have closely studied means of damaging or destroying the civilian communications networks of NATO member states, and it should be anticipated that this probing for vulnerabilities will intensify as relations deteriorate further. Russian president Vladimir Putin has repeatedly promised responses to Western actions that are unexpected and ‘asymmetric’.25 To prevent such responses, NATO governments should seek to minimize their self-inflicted vulnerabilities.

Nevertheless, unless adequately secured, 5G networks simplify the task of the attacker in achieving their aims. Examples include:

Network destruction and information interdiction. Adversaries can achieve effects remotely that currently require physical intervention against telecommunications infrastructure.26 This could be either in support of a localized objective, or a widespread attack in order to intimidate or blackmail victim states into political concessions.

Infiltration, espionage, and situational awareness. The substantial increase in the number of attack surfaces that must be protected will facilitate attempts at stealthy penetration of networks for the purpose of long-term surveillance and data collection.

Subversion and other sub-threshold attacks. The nature of 5G networks will introduce an additional layer of deniability to attacks on communications networks and connectivity, as attribution becomes more technically, and thus especially politically, complex.

In addition, the nature of 5G, as well as other advanced technologies’ reliance on it, presents adversaries with opportunities for the innovative exploitation of vulnerabilities. Cyber blackmail for political coercion is not a novel concept, but it takes on new dimensions thanks to the propagation characteristics of 5G. For demonstrations of the blackmailer’s capabilities, destruction of critical national infrastructure remains a relatively unlikely option, given the near-consensus that this constitutes an act of war. However, if such an attack were carried out, isolation measures intended to protect critical infrastructure would limit its reach. By contrast, more subtle interventions – like increasing the latency of the virtual network functions used for autonomous driving – allow less detectable operations but, at the same time, could affect much wider areas and spread throughout broad networks. In other words, rather than attacking an element of critical infrastructure, such as a water supplier, attacking a NFV will hit not just that one water supplier but any network operator using the NFV. And depending on the NFV (or any other software component crucial to the backbone), this may propagate rapidly and widely, including across borders – like a domino at a central junction.

#### New attack vectors expand the likelihood of and damage from cyberattacks on 5G connected infrastructure and devices.

Giles ’22 [Keir; 7/4/2022; Senior Consulting Fellow at Chatham House, Director of the Conflict Studies Research Centre, Fellow at the National Security Center of Excellence Canada; Kim Hartmann; Cyber and Information Technology Director at the Conflict Studies Research Centre; "Emergence of 5G Networks and Implications for Cyber Conflict," https://doi.org/10.23919/CyCon55549.2022.9810903]

5G Security Considerations

A proper grasp of the new security challenges presented by 5G requires an understanding of the highly complex technology involved. 5G networking introduces a number of technologies that political and strategic decision-makers may be unaware of but that are critical to understanding the risks incurred. These include the virtualization of hardware components, network slicing, software-defined networking, and the orchestration of these software components. All of these introduce CI/CD (continuous integration/continuous deployment) security aspects to network backbones, because the essential software will need to be developed and deployed continuously, opening up the backbones to CI/CD attack patterns.

CI/CD security is already an issue today, but usually this only affects software products – that is, a specific program, not the general backbone(s) of critical national infrastructure. Hence, CI/CD attacks have until now often only been relevant to software firms producing high-value targets, such as operating system developers. But in the same way as attacks against virtualized environments (considered further below), both the likelihood of attack and the profile of attackers are likely to change substantially due to the unprecedented nature of the 5G environment. An additional danger is that one attack pattern may be used to infiltrate the entire backbone; previously it was only able to attack a single software product. In effect, a single CI/CD attack against a suitable software component not only can be deployed against a wide geographical area but also, through a partially autonomous roll-out of updates, can easily and rapidly propagate to a wide variety of networks.

As ENISA states in its recent report on the 5G security landscape:5

One of the most important innovations in the 5G architecture is the complete virtualisation of the Core network… These novel network technologies and concepts that rely heavily on ‘softwarisation’ and virtualisation of network functions will introduce new and complex threats. The core network is the central part of the 5G infrastructure and enables all functions related to multi-access technologies. Its main purpose is to deliver services over all kinds of networks (wireless, fixed, converged).

A. Virtualization and Software-Based Architecture

At the core of the development of 5G lies the transition of several architectural components from previous hardware-based to software solutions. This transition has allowed the introduction of new functionalities that are crucial to meeting the demands that 5G networks were developed to address.

Virtualized network functions (VNFs) are used to provide services through software that replaces dedicated network devices. This shift from physical devices to software functions allows easier response and adaptation to environmental conditions (e.g. changes in network traffic or infrastructure). As such, they build the core of modern networks and are crucial to achieving the low latency and high speed of 5G networks which are currently being deployed. They build the new backbone of our upcoming networks. However, this makes VNFs of particular interest to cyber criminals, hacktivists, and state-sponsored hackers, especially as new attack vectors are introduced.

While virtualization does provide some means of inherent security, especially against attacks found on the lower end of technical capabilities, it also introduces new vulnerabilities, especially when expecting malicious actors from the higher end – dedicated, state-sponsored IT professionals paid to invade and infiltrate target networks. The particular threats that arise in 5G networks based on virtualization involve the possibility of ‘cross-contamination’ of shared hardware resources, the introduction of software components as basic network functions lacking integrity, and in general, the attack vectors associated with virtualization environments (e.g. such as hypervisor vulnerabilities and virtual machine escape attacks). Currently, it is anticipated that 5G network security to cope with virtualization attacks needs to be standardized and may be integrated fully based on existing solutions. However, the vast examples of attack vectors directed against virtualizations do make this approach questionable. Many of these attack vectors have been considered rather theoretical attacks in the past, as they required skilled personnel and financial resources. It was presumed that non-state actors were rather unlikely to make such an investment, especially as valuable targets usually combined virtual and physical security measures. This argument is no longer valid, since we must expect primarily state- and state-sponsored actors to attack the backbone of 5G networks and can no longer rely on physical security in 5G.

The fact that attack vectors against virtual environments are – compared to regular attacks experienced on networks today – relatively complex to carry out renders them even more likely to appear on 5G networks, as the attacker profile is likely to differ from today’s network attackers. This may change over time, but it is reasonable to expect that 5G networks will initially be a sector for high-skilled attackers rather than a playground for off-the-shelf exploits and ‘script kiddies’.

NFVs (network function virtualizations, a structure used for technical management and orchestration) are used to manage and orchestrate the virtualized basic, previously hardware-based, network functions. In order to do so, software components need to be addressable (in technical terms) in a standardized way. This is realized through inter-component interfaces, known as APIs (application programming interfaces). These APIs are challenging to design without introducing security vulnerabilities for a vast variety of technical reasons, whose explanation would exceed this article’s scope but which may be categorized as ‘API vulnerabilities’. Other expected vulnerabilities are account compromise, unauthorized (privileged) user access, unauthorized inspection or modification of data, and compromise of management and orchestration (MANO) components. This may lead to an invasion and subsequent control over the MANO module of the network and thus unauthorized control over all communication, functions, and operations performed through this network.6

#### Critical infrastructure disruptions ripple, causing extinction.

Dennis Pamlin & Stuart Armstrong 15, Dennis Pamlin, Executive Project Manager Global Risks, Global Challenges Foundation; Stuart Armstrong, James Martin Research Fellow, Future of Humanity Institute, Oxford Martin School, University of Oxford, “Global Challenges: 12 Risks that threaten human civilization: The case for a new risk category,” February 2015, Global Challenges Foundation, <https://www.pamlin.net/material/2017/10/10/without-us-progress-still-possible-article-in-china-daily-m9hnk>

Global Challenges – Twelve risks that threaten human civilisation – The case for a new category of risks 89

3.1 Current risks

3.1.5 Global System Collapse

Global system collapse is defined here as either an economic or societal collapse on the global scale. There is no precise definition of a system collapse. The term has been used to describe a broad range of bad economic conditions, ranging from a severe, prolonged depression with high bankruptcy rates and high unemployment, to a breakdown in normal commerce caused by hyperinflation, or even an economically-caused sharp increase in the death rate and perhaps even a decline in population. 310

Often economic collapse is accompanied by social chaos, civil unrest and sometimes a breakdown of law and order. Societal collapse usually refers to the fall or disintegration of human societies, often along with their life support systems. It broadly includes both quite abrupt societal failures typified by collapses, and more extended gradual declines of superpowers. Here only the former is included.

3.1.5.1 Expected impact

The world economic and political system is made up of many actors with many objectives and many links between them. Such intricate, interconnected systems are subject to unexpected system-wide failures due to the structure of the network311 – even if each component of the network is reliable. This gives rise to systemic risk: systemic risk occurs when parts that individually may function well become vulnerable when connected as a system to a self-reinforcing joint risk that can spread from part to part (contagion), potentially affecting the entire system and possibly spilling over to related outside systems.312 Such effects have been observed in such diverse areas as ecology,313 finance314 and critical infrastructure315 (such as power grids). They are characterised by the possibility that a small internal or external disruption could cause a highly non-linear effect,316 including a cascading failure that infects the whole system,317 as in the 2008-2009 financial crisis.

The possibility of collapse becomes more acute when several independent networks depend on each other, as is increasingly the case (water supply, transport, fuel and power stations are strongly coupled, for instance).318 This dependence links social and technological systems as well.319

This trend is likely to be intensified by continuing globalisation,320 while global governance and regulatory mechanisms seem inadequate to address the issue.321 This is possibly because the tension between resilience and efficiency322 can even exacerbate the problem.323

Many triggers could start such a failure cascade, such as the infrastructure damage wrought by a coronal mass ejection,324 an ongoing cyber conflict, or a milder form of some of the risks presented in the rest of the paper. Indeed the main risk factor with global systems collapse is as something which may exacerbate some of the other risks in this paper, or as a trigger. But a simple global systems collapse still poses risks on its own. The productivity of modern societies is largely dependent on the careful matching of different types of capital325 (social, technological, natural...) with each other. If this matching is disrupted, this could trigger a “social collapse” far out of proportion to the initial disruption.326 States and institutions have collapsed in the past for seemingly minor systemic reasons.327 And institutional collapses can create knock-on effects, such as the descent of formerly prosperous states to much more impoverished and destabilising entities.328 Such processes could trigger damage on a large scale if they weaken global political and economic systems to such an extent that secondary effects (such as conflict or starvation) could cause great death and suffering.

3.1.5.2 Probability disaggregation

Five important factors in estimating the probabilities of various impacts:

1. Whether global system collapse will trigger subsequent collapses or fragility in other areas.

2. What the true trade-off is between efficiency and resilience.

3. Whether effective regulation and resilience can be developed.

4. Whether an external disruption will trigger a collapse.

5. Whether an internal event will trigger a collapse.

[[CHART OMITTED]]

1. Increased global coordination and cooperation may allow effective regulatory responses, but it also causes the integration of many different aspects of today’s world, likely increasing systemic risk.

2. Systemic risk is only gradually becoming understood, and further research is needed, especially when it comes to actually reducing systemic risk.

3. Since systemic risk is risk in the entire system, rather than in any individual component of it, only institutions with overall views and effects can tackle it. But regulating systemic risk is a new and uncertain task.

4. Building resilience – the ability of system components to survive shocks – should reduce systemic risk.

5. Fragile systems are often built because they are more efficient than robust systems, and hence more profitable.

6. General mitigation efforts should involve features that are disconnected from the standard system, and thus should remain able to continue being of use if the main system collapses

7. A system collapse could spread to other areas, infecting previously untouched systems (as the subprime mortgage crisis affected the world financial system, economy, and ultimately its political system).

8. The system collapse may lead to increased fragility in areas that it does not directly damage, making them vulnerable to subsequent shocks.

9. A collapse that spread to government institutions would undermine the possibilities of combating the collapse.

10. A natural ecosystem collapse could be a cause or consequence of a collapse in humanity’s institutions.

11. Economic collapse is an obvious and visible way in which system collapse could cause a lot of damage.

12. In order to cause mass casualties, a system collapse would need to cause major disruptions to the world’s political and economic system.

13. If the current world system collapses, there is a risk of casualties through loss of trade, poverty, wars and increased fragility.

14. It is not obvious that the world’s institutions and systems can be put together again after a collapse; they may be stuck in a suboptimal equilibrium.

15. Power grids are often analysed as possible candidates for system collapse, and they are becoming more integrated.

16. The world’s financial systems have already caused a system collapse, and they are still growing more integrated.

17. The world’s economies are also getting integrated, spreading recessions across national boundaries.

18. The world’s political and legal systems are becoming more closely integrated as well. Any risk has not been extensively researched yet, and there remain strong obstacles (mainly at the nation state level) slowing down this form of integration.

19. The politics of the post-system collapse world will be important in formulating an effective response instead of an indifferent or counterproductive one.

20. System collapses can be triggered internally by very small events, without an apparent cause.

21. External disruptions can trigger the collapse of an already fragile system.

22. The trade-off between efficiency and resilience is a key source of fragility in a world economy built around maximising efficiency.

23. Climate change, mass movements of animals and agricultural mono-cultures are interlinking ecosystems with each other and with human institutions.

24. There is a lot of uncertainty about systemic risk, especially in the interactions between different fragilities that would not be sufficient to cause a collapse on their own.

#### Retaliation goes nuclear.

Klare ’19 [Michael; November; Professor Emeritus of Peace and World Security Studies at Hampshire College; Arms Control Association, “Cyber Battles, Nuclear Outcomes? Dangerous New Pathways to Escalation,” https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation]

Yet another pathway to escalation could arise from a cascading series of cyberstrikes and counterstrikes against vital national infrastructure rather than on military targets. All major powers, along with Iran and North Korea, have developed and deployed cyberweapons designed to disrupt and destroy major elements of an adversary’s key economic systems, such as power grids, financial systems, and transportation networks. As noted, Russia has infiltrated the U.S. electrical grid, and it is widely believed that the United States has done the same in Russia.12 The Pentagon has also devised a plan known as “Nitro Zeus,” intended to immobilize the entire Iranian economy and so force it to capitulate to U.S. demands or, if that approach failed, to pave the way for a crippling air and missile attack.13

The danger here is that economic attacks of this sort, if undertaken during a period of tension and crisis, could lead to an escalating series of tit-for-tat attacks against ever more vital elements of an adversary’s critical infrastructure, producing widespread chaos and harm and eventually leading one side to initiate kinetic attacks on critical military targets, risking the slippery slope to nuclear conflict. For example, a Russian cyberattack on the U.S. power grid could trigger U.S. attacks on Russian energy and financial systems, causing widespread disorder in both countries and generating an impulse for even more devastating attacks. At some point, such attacks “could lead to major conflict and possibly nuclear war.”14

#### Supply chain attacks cause global war.

Bradley Martin 21, Director of the RAND National Security Supply Chain Institute, and a senior policy researcher RAND Corporation, “Supply Chain Disruptions: The Risks and Consequences,” 11/15/21, https://www.rand.org/blog/2021/11/supply-chain-disruptions-the-risks-and-consequences.html

By now the impacts of supply chain disruption are becoming all too familiar: shortages, inflation, factory closures, goods waiting at ports to be unloaded. All these impacts are serious enough, but another more-hidden concern lurks just beneath the surface: the impact of supply chain failure on national security, broadly defined as a nation's ability to protect and ensure the well-being of its population.

This definition of “national security” is broader than just the defense industry or military-related efforts; it also could encompass the very ability of a nation to ensure economic well-being, public health, and protection of a nation's key infrastructure. Supply chain disruptions cause general economic disruption and key commodity shortages, which then in turn can, in fact, drive aggressive national behavior and international instability. And ironically, this reactive aggressive national behavior can happen even if the health of a national economy itself depends upon continued international economic interdependence. Indeed, this very interdependence can create vulnerabilities. So a systematic effort, cutting across agencies and public and private sectors, could be one way to ensure these vulnerabilities are understood and mitigated.

Supply Chain Disruption and Conflict

Dispersed supply chains develop because actors find it's economically advantageous to seek the least-expensive and most-productive sources of supply. These dispersed chains develop for good reasons, but they create complicated interdependencies whose risks and vulnerabilities are sometimes not even understood, let alone mitigated.

While the reasons for creating these chains lie largely with private interest, the effects of disruption—which can come from sources ranging from malign human action to natural disaster—are rarely localized. When shortages occur in one industry, the disruptions in one area nearly always spill into adjacent companies and sectors. Whole economies feel the impact, not isolated actors.

The impact on vulnerable populations may be particularly dire. Supply chain disruptions do not just create higher prices and shortages among high-end consumer products, such as cars. They also affect more-basic commodities such as generic drugs or energy, increasing the cost of living and the provision of basic needs.

This kind of disruption can create instability more generally, promoting conditions for conflict between and within nations. For the most part, nations try to maintain access to markets and resources by peaceful means such as stockpiling, direct investment in partner nations, and use of other financial incentives. However, there is no guarantee that such competition will remain peaceful.

As affluent nations and individuals can find ways to mitigate shortages, they may create blocs of “haves” and “have nots,” where some actors have enough but others cannot meet basic needs. “Haves” may find ways to more directly change distribution, most likely at the expense of other “have nots.” Or “have” nations may try to forcefully safeguard what they have gained and work to exclude competitors. In all these cases, the actors are facing shortages, occasioned by interdependence, and seeking security for themselves in ways that actually promote wider international systemic instability.

Escalation of Conflict

In some cases, supply chain disruptions can have an even more-direct impact than general disruption, causing shortages of commodities the nation must have to ensure national security. This kind of disruption can go beyond matters of justice, equity, and general prosperity to threatening a nation's very ability to defend itself and look after its citizens. Some examples are pharmaceuticals and personal protective equipment, energy, food, raw materials used in manufacturing, and semiconductors used in multiple different systems including military applications. Such shortages can make the need for a national government to act more dire and immediate and thus raise the risk of conflict. In some cases, particular types of raw materials only exist in certain places, so shifting to more-secure sources isn't even possible.

Supply chain disruptions create both leverage for some nations and reasons for other nations to minimize leverage. For example, Taiwan currently dominates the market for semiconductors, which in some respects gives it leverage with other actors, including the mainland People's Republic of China (PRC). Semiconductors are capital-intensive—a new fabrication facility for semiconductors costs approximately $4 billion, with some estimates as high as $12 billion, and can take three or more years to build.

This does not even account for the skilled labor, and points to the difficulty of readily shifting production. As a result, Taiwan gains considerable leverage over the PRC and indeed the world. However, this very dominance, plus its proximity to the PRC and its dependence on the PRC for other commodities, may in fact raise the incentive for the PRC to take aggressive military action to ensure access to a key commodity. Such action could range from a “quarantine” to military threats to an actual invasion.

Aggressive action may stop well short of outright war, yet still be very dangerous for actors in the system. The problem of security vulnerability overall is complicated by the complexity and spread of supply chains across the world. A nation might not be able to successfully secure a commodity just by aggressive action against a single other nation. However, that action against another nation certainly could have the unintended effect of causing supply chains to fail in a more general manner. Aggressiveness, while understandable and probably predictable, might therefore also be extremely dangerous and unproductive.

Conflict and Instability

Nations have gone to war in the past over natural resource shortages or in an effort to secure key markets and labor pools. The need to secure resources and markets was an explicit premise in German and Japanese actions leading to World War II. Such conflict has occurred even during times of significant interdependence between nations, such as in the European system prior to World War I. Historically, nations have not yet resorted to war to ensure supply chain security, but it might be a mistake to assume that such action could never occur when circumstances become sufficiently dire. Interdependence does create incentives to cooperate to avoid disruption, but may offer few alternatives for some desperate nations if some part of the interdependent chain is broken.

#### Without cyber-secure 5G, NATO risks tech leadership, failed smart cities and IP theft. 5G is key----it’s the critical enabler of all emerging systems.

Jones ’20 [James; 10/1/2020; former commander of U.S. European Command and Supreme Allied Commander, Europe; "NATO Future, 5G and Cyber Security with General James L. Jones, Honorary President of SESC," https://sesecuritycenter.org/nato-future-5g-and-cyber-security-with-general-james-jones-president-of-sesc-advisory-board/]

These enormous leaps in human capability are poised to transform nearly every aspect of how we live, work, play, and defend ourselves. How these innovations develop, and under whose leadership, will have much to say about the future balance of economic power and global geopolitical influence now and in the decades to come.

At the core of this emerging period of new life-altering technology- a singular technology pulling it all together and making it possible- is the next generation of wireless communications networks- known as 5G.

While 4G was evolutionary, the speeds and capacities provided by 5G networks will be disruptive and revolutionary… and not just because they will make our cell phones better and our Internet connections faster. 5G will be the central nervous system harnessing the sensors, communication links, computing capacity and learning that will make everybody, everything, and everyplace smarter and more functional.

The country or group of countries that roll out the network quickest and best will enjoy a first mover advantage in developing the innovation-related goods, services, and solutions. It will also create a new category of jobs. Prosperity enables us to secure ourselves, fulfill our commitments to our friends and allies, and advance the nation’s interests and values.

The great power winner of this race will have the upper hand in setting global 5G norms and standards. Nothing could be more consequential in how the global future takes shape. By the way, welcome back to a new bipolar world, this time U.S.- China. Russia is a declining power, and is more of a strategic nuisance than anything else, with Vladimir Putin to blame.

Under China’s model and behavior, precedent informs us that 5G capabilities will be employed to steal intellectual property, monitor and control its population, and control as much of the global data as possible. Conversely, the US and allied model for 5G will be a platform to empower and protect the privacy of the individual, protect intellectual property, and safeguard national secrets, all the while enabling growth and development.

Consider that China is clearly subsidizing the sale of its 5G equipment which enables a pricing policy that is at least 40% less expensive than ours. China has the strategic goal of entrenching its network equipment into the systems that operate the world’s critical infrastructure. One can think of it as the digital belt and road strategy- and many countries are falling for what amounts to a very seductive, but ominously dangerous, strategy.

Unfortunately, we have every reason to believe that, among other things, China sees the deployment of its 5G equipment as commercial intelligence platforms, data syphons and digital sleeper cells sitting at the heart of nation-critical systems across the globe. The digital backdoors and remote-alterable software they contain give China an enormously powerful chokehold- in which 5G can serve as fifth column.

There is good news: the transition to 5G provides the United States, our friends, and allies a golden opportunity to build greater cybersecurity into our networks by improving our supply chain practices and creating more responsible and enforceable global norms.

Making these improvements is crucial to protecting our qualitative military edge, securing command, control and communications networks, achieving greater interoperability, and better protection of our critical infrastructure, as well as safeguarding personal privacy.

But unless the transition is not just to 5G but to Secure 5G, the future will be one of increased vulnerability and insecurity. There will be no smart cities without a secure network, and there will be no protection of security, intellectual property, or privacy for the individual.

We are going to enter the 5G world, of this there is little doubt. 5G technology is the current generation’s “(1957) Sputnik moment,” a time when the headlines could soon announce that China has won the race to 5G over the US and its allies.

#### Chinese-led order immediately causes extinction and upends liberalism.

Wang ’19 [Fei-Ling; October 24; Professor at the Sam Nunn School of International Affairs, Ph.D. from the University of Pennsylvania; The Cipher Brief, “The China Order: A Challenge for the U.S. and the World,” <https://www.thecipherbrief.com/column_article/the-china-order-a-challenge-for-the-u-s-and-the-world>]

It is no longer hard to see that the rising power and the mounting pugnaciousness of the People’s Republic of China (PRC) have become a comprehensive challenge for the United States. China’s Machiavellian policies and actions at home and abroad have turned an otherwise naturally complementary Sino-American economic relationship into a near zero-sum, if not already a zero-sum, competition for market, jobs, technology, and financial primacy. Beijing now openly flexes its new muscles in its neighborhood and beyond to resist, reduce, and replace American leadership and presence everywhere possible, seeking to undermine the U.S.-led international economic order and American-anchored collective security arrangements. The PRC has been burning billions, for example, hoping to replace the U.S. dollar with the over-printed Chinese Renminbi (RMB). Extraordinarily heavy extraction of its own economy, the world’s second largest, and its enormous foreign currency reserve resulting from the gross imbalance in U.S.-China trade have enabled the PRC to massively expand its military. That military is already the world’s second largest; its navy, for example, is projected to soon surpass the U.S. Navy in fleet tonnage. At the same time, massive but opaque spending sprees has allowed the PRC to actively procure power and proxies even inside the United States, positioning Beijing to reshape international opinions and norms more easily than ever.

What is less known, perhaps, is that the rising PRC state also seeks an overhaul of the very world order that has enabled the greatest advances of human civilization over the past few centuries – the Westphalian system of nation-states. This world order was codified in the 17th century, expanded to a global scale in the 20th century, and now is in its post-World War II and post-Cold War iteration — the so-called America-led Liberal International Order (LIO). The rise of Chinese power, under the autocracy of the Chinese Communist Party (CCP), is not just contesting U.S. national security and American global leadership but also the existing world order. Never since the heyday of the Cold War has the world seen such a full challenge to the United States and to the Westphalian system.

The CCP is leading the PRC toward a Chinese Dream of a world order in its own image, which I call the China Order. The China Order is a millennia-old political tradition and ideology that mandates a unitary, authoritarian (often totalitarian), omnipotent and omnipresent government for the whole known world. This alternative world order has had a variety of euphemisms in the long history of China: from tinaxia yitong (unification of all under heaven) and shijie datong (world’s grand harmony) in the imperial past, to Mao Zedong’s world solidarity for Communist revolution only forty years ago, to now Xi Jinping’s community of common human destiny. The China Order has powerfully revived to guide rising PRC power, under the banner of a Chinese version of globalization, ingeniously taking advantage of the various calls in our time for global governance to address transnational issues such as climate change, inequality, epidemics, and terrorism.

This China Order is normatively and practically at fundamental odds with the LIO version of the Westphalia system that enshrines comparison and competition among nations coexisting with equal sovereignty. The China Order has been widely addictive to the powerful and ambitious in history, whether they have been ethnically Han or not. It has been highly effective in practice, in great part because it became deeply legitimized and internalized in elite Chinese culture over many centuries. The China Order is now the sole acceptable model of the world under the authoritarianism known as the Qin-Han polity that the PRC now practices. But under this world order, as documented by The China Order (#ad), human civilization is socio-economically very suboptimal and hopelessly stagnant, inevitably shortchanging the lives of just about everyone, especially nonelites, as the tragic and often catastrophic history of Eastern Eurasia under the China Order before the nineteenth century amply demonstrates.

Since 1949, when the PRC restored traditional Chinese autocracy under the guise of imported Marxism-Leninism, the CCP has been ceaselessly and callously fighting its own people internally and the United States and American allies externally to preserve its monopoly over power. Only sheer exhaustion and near collapse could force the CCP to slow down and retreat, at home and abroad. External powers have influenced and facilitated the rise of PRC power, but have so far failed to transform the Qin-Han autocracy and its China Order ideal, thus remaining unable to change Beijing’s world views and global pursuits. Various, often false, rationalizations have justified the continuation of American/Western engagement with the PRC, which has greatly enriched and enabled the CCP to persist in its consolidation of power. Beijing’s push for power is nothing personal; it is a brand of authoritarianism just happens to be anchored in the remarkably persistent belief that failing to achieve control over the whole known world would spell the loss of the “mandate of heaven” and political extinction. Thus, the CCP is driven (or doomed) to methodically and opportunistically seek ever greater influence.

The rise of China, or more precisely the ever-greater power of the PRC state, represents a shift of the distribution and concentration of power in the international system (conceptually known as power transition) and an effort to reorder the units in the system and change the system’s governing norms. Chinese leaders have already openly claimed that they are now moving to the center of the world stage, leading a revolutionary change in the world order, upending the Peace of Westphalia established “four hundred years ago,” in the words of PRC leaders This points to a systemic change of world politics and a choice for all of us at the grandest possible scale: a scale that could reshape nations and redirect the path of human civilization. The PRC’s challenge is therefore greater than the struggle between the two European ideologies of Capitalism and Communism. The confrontation between the U.S.-led LIO and the PRC-dreamed China Order transcends these often vaguely defined civilizational clashes.

If the PRC challenge, the rise of an unscrupulous, ever more resourceful and determined PRC state, is not managed well and promptly, the United States will have to face a much worse choice in the not too distant future between tragic capitulation and a desperate war for its national security and world leadership and for the way in which humankind is organized worldwide. In the age of many kinds of weapons of mass destruction, this will be a harrowing decision.

Of course, one may argue that the grandiose China Dream of a China Order may be just another pretentious way for the CCP to invoke traditional, nationalist, and populist ideals to justify its autocratic governance of the Chinese people forever, similar to the splendid slogans and missions fabricated by many other dictators. Perhaps the highly insecure CCP leadership is fighting for its survival, not world domination. However, words have consequences. Propaganda and dilution often greatly mesmerize and mislead the pretenders themselves. More importantly, the CCP has been steadily following up its words with action and money for years (basically nonstop since 1949); it has just pledged over 10 times the total sum of the Marshall Plan (in today’s dollars) for its Belt and Road Initiative alone, for instance.

As the logic of the China Order dictates, the rising Chinese power will not stop short of unseating the United States and reordering the world, unless Beijing’s Qin-Han polity is transformed and/or the ever richer and more powerful PRC is checked. The alternatives, American capitulation or world war, are horrific to contemplate, but not necessarily impossible. Unlike in Hollywood, the “good” guys do not always win necessarily in the real world. A mighty autocracy that tightly controls one-fifth of humankind, willfully spends a disproportionately larger portion of the fruits of the world’s second largest economy, and vows (even if only hypocritically) to reform and reorder the world under its leadership, is and will always be a mortal challenge to the national security of the United States. America’s global position and way of life, world peace, and the overall world order all rest on how the PRC challenge is managed—soon.

#### IP theft undermines innovation necessary for global problem solving---extinction.

Rando ’16 [Robert; June 2016; Partner at Greenspoon Marder LLP, concentrating in Intellectual Property Law, J.D. from St. John’s University School of Law; "America’s Need For Strong, Stable and Sound Intellectual Property Protection and Policies: Why It Really Matters," https://randolawfirm.com/uploads/3/5/3/6/35367334/ip\_insight.pdf]

Without engaging in “chicken and egg” analysis, it is sufficient to observe that technological advancement, societal needs, globalization, existential threats, economic realities, and political imperatives (or what James Madison referred to in the Federalist Papers No. 10 as factious governance), have combined to create the “interesting times” for the United States [IP] intellectual property laws.

What was said by Bobby Kennedy in 1966 remains true today. We live in dangerous and uncertain times. Many of the existential threats remain the same (nuclear war and proliferation, [genocides] genocidal maniacs and natural disease) and some are new ([hu]manmade disease, greater awareness of environmental changes and possibly human interrelationship factors, and the unintended consequences of genetic manipulation and robotic technologies). The danger and uncertainty that pervades changes in intellectual property laws, though not an existential threat of the same manner and kind, correlates with the threat and remains “more open to the creative energy of man than any other time in history.”

Apropos the creative energy of man, there is a non-coincidental congruence and convergence of activity across and among the three branches of government, occurring almost simultaneously with the congruence and convergence of the rapid developments of technological innovation across various scientific disciplines and the information age, reflected in the transformation of the [IP] intellectual property laws in the United States.

Patents

The passage of the AIA was a culmination of efforts spanning several years of Congressional efforts; and the product of a push by the companies at the forefront of the twenty-first century new technology business titans. The legislation brought about monumental changes in the patent law in the way that patents are procured (first inventor to file instead of first to invent) and how they are enforced (quasi-judicial challenges to patent validity through inter-party reviews at the Patent Trial and Appeals Board (PTAB)).

The 113th and 114th Congress grappled with newly proposed patent law reforms that, if enacted, may present additional tectonic shifts in the patent law. Major provisions of the proposals include: fee-shifting measures (requiring loser pays legal fees - counter to the American rule); strict detailed pleadings requirements, promulgated without the traditional Rules Enabling Act procedure, that exceed those of the Twombly/Iqbal standard applied to all other civil matters in federal courts, and the different standards applicable to patent claim interpretation in PTAB proceedings and district court litigation concerning patent validity.

The Executive and administrative branch has also been active in the patent law arena. President Obama was a strong supporter of the AIA3 and in his 2014 State Of The Union Address, essentially stated that, with respect to the proposed patent law reforms aimed at patent troll issues, we must innovate rather than litigate.4 Additionally, the USPTO has embarked upon an energetic overhaul of its operations in terms of patent quality and PTO performance in granting patents, and the PTAB has expanded to almost 250 Administrative Law Judges in concert with the AIA post-grant proceedings’ strict timetable requirements.

The Supreme Court, not to be outdone by the Articles I and II branches of the U.S. government, has raised the profile of patent cases to historical heights. From 1996 to the 2014-15 term there has been a steady increase in the number of patent cases decided by the SCOTUS5. The 2014-15 term occupied almost ten percent of the Court’s docket. Prior to the last two decades, the Supreme Court would rarely include more than one or two patent cases in a docket that was much larger than those we have become accustomed to from the Roberts’ Court6.

While the SCOTUS activity in patent cases is viewed by some as a counter-balance to the perceived Federal Circuit’s pro-patent and bright line decisions, it can just as assuredly be viewed as decisions rendered by a Court of final resort which does not function in a vacuum devoid of the social, economic and political winds of the times. In recognition of the effect new technologies have on the patent law, the politicization of intellectual property law matters, especially patent law (through factious governing principles of the political branches of the government), and the maturation of the Federal Circuit patent law jurisprudence, the SCOTUS has rendered opinions in cases that impact, and perhaps are/were intended to mitigate the concerns regarding, some of the vexing issues confronting the patent community today (e.g., non-practicing entities or in the politicized parlance “patent trolls,” the intersection of patent and antitrust laws in Hatch-Waxman so called “pay-for-delay” settlements between Branded and Generic pharma companies, and the fundamental tenets that comprise the very heart of what is patent eligible subject matter).

Copyrights

The advent and ubiquity of the internet, social media and digital technologies (MP3s, Napster, Facebook, YouTube, and Twitter) represents the impetus for changes in the Copyright laws. The DMCA addressed the issues presented by these advances or changes in the differing media and forms of artistic impressions. The proliferation of digital photos, graphic designs and publishing alternatives, as well as adherence to globalization harmonization have given rise to changes in the statutory law and jurisprudence in this area of intellectual property law. Additionally, there is an overlap of patent rights and copyrights for software driven by the ebb and flow of the strength of each respective intellectual property protection.

Notably, the Patent and Copyright Clause7, in addition to Author’s writings, has been viewed as discretely applying to two different types of creativity or innovation. When drafted the “sciences” referred not only to fields of modern scienctific inquiry but rather to all knowledge. And the “useful arts” does not refer to artistic endeavors, but rather to the work of artisans or people skilled in a manufacturing craft. Rather than result in ambiguity or confusion, perhaps the Framers were either quite prescient or, just coincidentally, these aspects of the Patent and Copyright Clause have converged.

For example, none other than the famous Crooner, Bing Crosby, benefited from both protections. Well-known as a prolific and popular recording artist he also benefited from his investments in the, then innovative, recording technologies. Similarly, the Beatles, Beach Boys, as well as many other rock and roll artists, experimental efforts in music performance, recording and production, helped to transform the music industry in both copyrightable artistic expression and patentable inventions. Similarly, film, literary and digital arts reap benefits at the crossroads of both copyright and patent protections.

Trademarks

Trademark laws have been impacted by numerous changes in the business landscape. They include the internet, Domain names, international rights in a global economy, different venues and avenues for branding, marketing and merchandising, global knock-offs from nations that have a less than stellar respect for intellectual property rights, and international trade agreements. More recently, politicization (or perhaps political correctness) has creeped into the trademark law arena pitting branding rights and protections against first amendment rights.

Trade Secrets

As with Copyright and Trademark law, trade secrets law includes some of the same issues related to trade agreements. TRIPS required members to have trade secret protection in place. Initially, the United States compliance with this requirement has relied upon the trade secret law of the individual states. That compliance may be supplanted by the recently enacted DTSA. Similarly, the Trans Pacific Partnership (TPP) trade agreement contains intellectual property rights provisions that will trigger required changes to United States statutory Intellectual Property Laws.

The proposed trade secret legislation also gives rise to several concerns. For instance, there is an absence of a specific definition for trade secret, as well as potential issues of federalism, conflict with state law precedent (despite no preemption), remedies, and the impact on employer/employee relations.

There is also a real concern that the strengthening of trade secret protection in conjunction with the perceived weakening of patent protection (e.g., high rate of invalidating patents in post-grant proceedings before the PTAB and strict limitations on what is patent eligible subject matter) may very-well have the unintended consequence of contravening the purpose behind the Patent and Copyright Clause: “to promote the progress of the sciences and the useful arts.” Moreover, the incentive to innovate may very well be usurped by the advantage of withholding patent law disclosure of highly beneficial scientific advancements that directly affect the human condition, alter life expectancies and the evolution of the human species (rather than by mere “natural selection”), and what is the very essence of a human being (for better or worse). Thus, crippling innovation and the progress of the sciences and useful arts.

Privacy Rights

It is increasingly more difficult to function “off the grid.” The invasive and non-invasive attributes of the internet, the reliance upon the multitude of devices, social media, and information age technologies, and access to big data, all contribute to the decrease in and dilution of the right to privacy. Wittingly or otherwise, the strong libertarian roots of the republic have been replaced by dependence upon these modes of an information-age life. Commentary on the benefits and deficits of this reality are beyond the subject and purpose of this writing. Suffice to acknowledge that the right to privacy has been significantly reduced. The laws that protect these rights are in a constant struggle to maintain those rights while yielding to the demands of the lifestyle and security concerns. Laws that relate to cybersecurity in the global and domestic space create interplay with privacy rights. Legislation, trade agreements and jurisprudence all impact this area of intellectual property. Cross-border theft of trade secrets, competitor espionage, and loss of control over personal data are all implicated in the intellectual property law arena.

America’s Need For Strong Intellectual Property Protection

The need for strong protection of intellectual property rights is greater now than it was at the dawn of our republic. Our Forefathers and the Framers of the U.S. Constitution recognized the need to secure those rights in Article 1, Section 8, Clause 8. James Madison provides insight for its significance in the Federalist Papers No. 43 (the only reference to the clause). It is contained in the first Article section dedicated to the enumerated powers of Congress. The clause recognizes the need for: uniformity of the protection of IP rights, securing those rights for the individual rather than the state; and, incentivizing innovation and creative aspirations.

Underlying this particular enumerated power of Congress is the same struggle that the Framers grappled with throughout the document for the new republic: how to promote a unified republic while protecting individual liberty. The fear of tyranny and protection of the “natural law” individual liberty is a driving theme for the Constitution and throughout the Federalist Papers. For example, in Federalist No. 10, James Madison articulated the important recognition of the “faction” impact on a democracy and a republic. In Federalist No. 51, Madison emphasized the importance of the separation of powers among the three branches of the republic. And in Federalist No. 78, Alexander Hamilton, provided his most significant essay, which described the judiciary as the weakest branch of government and sought the protection of its independence providing the underpinnings for judicial review as recognized thereafter in Marbury v. Madison.

All of these related themes are relevant to the Patent and Copyright Clause and at the center of the intellectual property protections then and now. The Federalist Papers No. 10 recognition that a faction may influence the law has been playing itself out in the halls of congress in the period of time leading up to the AIA and in connection with the current patent law reform debate. The large tech companies of the past, new tech, new patent-based financial business model entities, and pharma factions have been the drivers, proponents and opponents of certain of these efforts. To be sure, some change is inevitable, and both beneficial and necessary in an environment of rapidly changing technology where the law needs to evolve or conform to new realities. However, changes not premised upon the founding principles of the Constitution and the Patent and Copyright Clause (i.e., uniformity, secured rights for the individual, incentivizing innovation and protecting individual liberty) run afoul of the intended purpose of the constitutional guarantee.

Although the Sovereign does not benefit directly from the fruits of the innovator, enacting laws that empower the King, and enables the King to remain so, has the same effect as deprivation and diminishment of the individual’s rights and effectively confiscates them from him/her. Specifically, with respect to intellectual property rights, effecting change to the laws that do not adhere to these underlying principles, in favor of the faction that lobbies the most and the best in the quid pro quo of political gain to the governing body threatens to undermine the individual’s intellectual property rights and hinder the greatest economic driver and source of prosperity in the country.

It is also important to recognize that the social, political and economic impact of strong protections for intellectual property cannot be overstated. In the social context, the incentive for disclosure and innovation is critical. Solutions for sustainability and climate change (whether natural, man-made or mutually/marginally intertwined) rely upon this premise. Likewise, as we are on the precipice of the ultimate convergence in technologies from the hi-tech digital world and life sciences space, capturing the ability to cure many diseases and fatal illnesses and providing the true promise of extended longevity in good health and well-being, that is meaningful, productive, and purposeful; this incentive must be preserved.

In similar fashion, advancements in technologies related to the global economy and communications will enhance the possibilities for solutions to political and cultural conflicts that arise around the globe. Likewise, the United States economy has always benefited when it is at the forefront of innovation and achieves prosperity from its leadership role in technological advancements.

Conclusion

As was the case in 1966, how we move forward today, to solve the many problems facing our country and the broader global community in these “interesting times,” both within and without the laws affecting intellectual property rights, depends upon the “creative energy of man” which must prevail. An achievable goal, dependent on the strong, stable and sound protection of intellectual property rights.

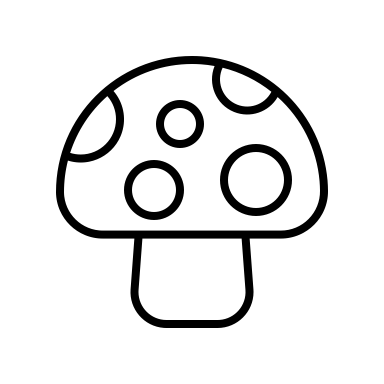
#### Cyber risks to smart cities are existential but securing them solves.

Robert Muggah 21, principal at the SecDev Group and co-founder of the Igarape Institute; and Greg Walton, fellow at the SecDev Group and a researcher at the Oxford Internet Institute, 4/17/2021, "‘Smart’ Cities Are Surveilled Cities," Foreign Policy, <https://foreignpolicy.com/2021/04/17/smart-cities-surveillance-privacy-digital-threats-internet-of-things-5g/>, RMax

But a narrow preoccupation with surveillance technologies, as disconcerting as they are, underestimates the threats on the near horizon. Smart cities are themselves a potential liability—for entirely different reasons. This is because many of them are approaching the precipice of a hyperconnected “internet of everything,” which comes with unprecedented levels of risk tied to billions of unsecured devices. These don’t just include real-time surveillance devices, such as satellites, drones, and closed-circuit cameras. By 2025, there could be over 75 billion connected devices around the world, many of them lacking even the most rudimentary security features. As cities become ever more connected, the risks of digital harm by malign actors grow exponentially. Cities are therefore entirely unprepared for the coming digital revolution.

One of the paradoxes of a hyperconnected world is that the smarter a city gets, the more exposed it becomes to a widening array of digital threats. Already, large, medium, and small cities are being targeted for data theft, system breaches, and cyberattacks, all of which can undermine their operation and provision of essential services, and pose an existential threat. Hundreds of cities around the world have reported major digital disruptions to municipal websites, emergency call centers, health systems, and utilities delivering power or water. When city security is compromised and data privacy jeopardized, it undermines the faith of residents in digitally connected services and systems. As people feel more insecure, they may feel less inclined to participate in online health care, digitized utilities, remote learning opportunities, electronic banking services, or green initiatives—key tenets of the smart city. While not all digital threats can be countered, cities need to mount a robust capability to deter, respond to, and recover from attacks while preserving, as best they can, data protection and privacy.

#### Coordination within NATO secures 5G supremacy and ensures global cooperation towards secure 5G.

Danielle McDonald 21; M.A. in History from the University of Waterloo and Senior Business Funding Analyst at Mentor Works: The Government Funding Planners; "5G: Geopolitics, Global Competition & NATO ," 5G: Geopolitics, Global Competition & NATO, 05/07/2021 <https://www.turkheritage.org/en/nato-resource-center/nato-publications/5g-geopolitics-global-competition--nato--9688//>

What is 5G?

Magnifying the proficiency of modern-day technology is the fifth-generation cellular wireless network, 5G. Like the preceding generation launches of mobile networks, 5G enables numerous capabilities through greater capacity, shorter wavelengths, worldwide mobile internet connections, and high-frequency bandwidths [1]. As part of telecommunication networks, 5G technology expands the productivity of correspondence between machines without human assistance [2]. Such improvement grants 5G as the foundation for advancements in autonomous cars, smart roads, Augmented Reality (AR), intelligent healthcare and medicine, and semi-autonomous robots for everyday use [3].

In detail, there are three cross-cutting components to the essence of 5G. These are increased efficiency, multipath ways, and swift signal delivery across the 5G spectrum for core network functions [4]. What is significant is that the framework is software-based, and any adjustments can be made through a simple software update or replacement, if necessary [5]. Certainly, abilities such as that of 5G are costly to implement, which brings both possibilities and complications to the idea of network sharing to decrease expenses.

Nonetheless, the incorporation of 5G into modern and future technologies is making momentous progress in both individual and company life. This kind of technology will be significantly impactful for consumers in areas such as retail, entertainment, automotive production, the manufacturing industry, and logistical processes [6]. Likewise, it will have an incredible stake in government and national security. 5G is already integral in ongoing technological advancements and security strategies for actors in the global political economy.

Technology and Geopolitical Relations: Will the bifurcation of the technology world posit better relations?

Along with 5G, other technological developments such as Artificial Intelligence (AI), robotics, and nanotechnology are powerful tools of influence in economic and trade interests. Many scholars and scientists claim that this new technology is changing the geopolitical landscape [7]. There is already a gap between developed and developing countries in obtaining new technologies [8]. Should the unequal access in the digital world continue, developing countries are bound to keep further behind which can ultimately stifle progress to development.

At the forefront of technology and geopolitics concerns is the anomaly that new technology is bringing about profound social change in data localization [9]. Significantly, it is altering the distribution of power, broadly in western democratic and authoritarian regimes [10]. Thus far, in democracies, there has been an increase in power at the individual citizen level and a decrease in state power [11]. On the contrary, authoritarian regimes are experiencing an increase in state power and a decreased power of citizens [12]. As the ambiguity of experiencing different trends persist, it becomes prudent to ask oneself how this may affect future trade relations, tensions in the global technological competition, and success in adopting policies and standards worldwide.

China in the 5G Equation

China boasts a competitive advantage over foreign markets as it has accumulated expertise and experience since the introduction of 5G networks. Due to high levels of industrialization, low costs of production, and domestic and foreign market supply and demand, the maturity and sophistication of Chinese companies have dubbed it as the leader in the global race to obtain and develop 5G technology [13].

The Chinese company Huawei has emerged as a powerhouse in the world’s telecommunications infrastructure [14]. Part of the concerns about China’s rising influence is due to its capacity to present weaknesses through software updates and the ability to use competitive prices to insert itself into the fundamentals of capitalistic democratic societies [15]. Seeing that the Chinese government does not encourage a free market but rather exerts control over its companies, this poses a great cybersecurity threat to states’ national security as sensitive information that can be accessed from the simplest online interaction by China. To date, both the United States and the United Kingdom have banned Huawei from their networks due to concerns of security. A rise in leadership from a Western alternative in opposition to Huawei has been a challenge because Huawei and ZTE, both China-based companies, were major suppliers of 4G networks.

In an attempt to further increase its influence through the digital markets, China has launched the Digital Silk Road (DSR) which is a very integral part of the overall Belt and Road Initiative (BRI) strategy. An essential component of the DSR strategy is to finance other countries’ telecommunications infrastructures. This is one of the main ways that Chinese firms have built their 5G network and technology standards in other countries, therefore posing the risk of potential espionage and involvement in internal state legislative issues [16]. Nonetheless, recipient countries of China’s 5G firms have attained a greater aptitude to filter and moderate content, localize data and surveil the digital world [17].

NATO: 5G’s challenges and opportunities

China’s digital footprint in 5G brings the potential of future military development into perspective. China is known to have aggressive tensions with the NATO Alliance members, therefore sparking a need for more cohesion. Since the development of 5G, NATO and its allies have not been playing major roles in the newest telecommunications software. To best comprehend NATO and how it can obtain and develop 5G for a secure, responsible global environment, it is best to analyze 5G in three essential ways.

Firstly, 5G needs to be seen as an area for development. Any introduction of new technology allows for discussion which can better help allies to comprehend the complexities and need for policies for technological transitions [18]. Increasing economic growth through such technology also results in the need to execute command and control, manage communications, artificial intelligence, and cloud computing behind the scenes and on the battlefield [19]. Doing so will not only allow for room for development but will overall enhance the quality of military equipment needed to achieve NATO goals.

Moreover, a second way that 5G needs to be viewed is as an ecosystem that needs to be protected. Being a telecommunications network that is a hyper interconnective system, it is something that private and government sectors struggle to find a common ground on for its operations and policies [20]. If not protected in both playing fields, next-generation telecommunications will run into a vast array of problems and security insecurities. In addition, because 5G operates on machine-to-machine communication, the perimeter cyber defense is ineffective [21]. As risks of cyber-attacks grow, NATO needs to ensure that their 5G development efforts take into consideration that integrating equipment from Chinese firms widens and deepens serious questions of trust and reliability for military functions [22]. Consequently, if the 5G ecosystem is not protected, then serious political ramifications can occur as a result. Aforementioned, the value of privacy is different in China than it is in western democracies. Chinese government’s direct access to its firms poses advantages to the Chinese intelligence community which, in turn, will prompt countries to reconsider their methods in storing big data [23]. Being at odds with a country due to differences in privacy laws, democratic values and ethics are very important because they can potentially constrain relations.

Because of the world’s interdependence on 5G networks, it poses a suitable avenue for collaboration amongst NATO allies and with countries outside the transatlantic alliance. The world of telecommunications takes on the concept that “the early bird gets the worm.” Demonstrated in China’s leadership of 5G development, most state actors still have a strong motivation to merge into the race and assume a position that could amplify their economy [24]. It should be understood that telecommunication is truly strategic in nature. Working together to ensure speed and the quality and quantity of information is a multifaceted avenue for the Alliance, its allies, and non-members to engage in healthy global cooperation.

### Military 5G---1AC

#### Advantage 2 is Military 5G.

#### Military 5G deployment is inevitable but compromised by lack of cybersecurity and interoperability.

Emma Helfrich 21, technology editor at Military Embedded Systems; quoting Lance Spencer, client executive vice president for defense at AT&T Public Sector and FirstNet; Craig Miller, president of ViaSat Government Systems; and John Cowles, director of engineering and technology at Analog Devices, 10/19/2021, "5G and the military: A new era of connectivity," No Publication, <https://militaryembedded.com/comms/communications/5g-and-the-military-a-new-era-of-connectivity>, RMax

Fifth-generation wireless technology, or 5G, is poised to emerge in a big way into the defense market. While the buzz surrounding the 5G technology standard has been growing in the general public in recent years, the U.S. Department of Defense (DoD) has been trailing behind commercial entities on adopting 5G due in part to both the slower pace of the DoD’s acquisition process and the hard-to-keep-up-with pace of consumer-technology refresh. However, officials at several defense communications companies agree that it’s just a matter of time before 5G-enabled military solutions are deployed and forever change the way in which the armed forces communicate.

That fact that 5G is a largely commercially developed solution that is now on track for adaptation to military use has enabled defense electronics manufacturers to operate in collaborative environments. This reality will prove to be valuable, as one of the driving factors behind widespread 5G adoption in the military is not the advent of the waveform itself, but the set of network-management standards that will follow.

Multidomain operations, as seen in military programs such as Joint All Domain Command and Control (JADC2), could greatly benefit from the interoperability enabled through 5G use. One way is through 5G technology’s ability to bring disparate solutions together under a unified network management system.

With 5G adoption occurring all around the world, electronic warfare (EW) and spectrum-management applications could also see an evolution following the implementation of 5G architectures. The use of 5G and its incorporation into intelligence, surveillance, and reconnaissance (ISR) systems could indelibly alter how the military gathers actionable intelligence, ranging from how the DoD detects/is detected to further opening vast avenues of data collection.

The transition from Long Term Evolution 4G (4G LTE) to standalone 5G deployment will be gradual, just as it was from the early days of 1G (launched in Japan in 1979, adopted in 1983 in the U.S.) all the way to December 1, 2018, when South Korea became the first country to offer 5G. The process will take even longer to reach the military, with networking standards, current DoD networking architectures, and measured acquisition timelines among the current hurdles bogging down immediate fielding.

The difference between 4G and 5G

Following the introduction and implementation of 4G LTE in consumer and military markets, the unprecedented streaming ability that it offered was regarded as revolutionary. While patchiness in the 4G LTE network did leave users in certain regions unsatisfied, it’s a fact that 5G was already in the planning stages.

“5G, as it actually came to be, was thought of as more than just a generational change in how we communicate through a cellular environment with cell phones. It was actually pretty far-reaching in its genesis,” says John Cowles, director of engineering and technology at Analog Devices (Wilmington, Massachusetts). “It’s more than a comms system, as it enables a system of different systems. What I mean by that is there’s a traditional cellphone system, but 5G also envisions how that might affect IoT [Internet of Things], or even satellite communications. There’s terrestrial communication, there’s people, there’s data, there’s IoT, and then there’s the satellite piece of it.”

Often referred to by industry professionals as the IoT era, 5G dawned amid the understanding that data was being created far more quickly and in volumes greater than what current networks could handle. The vast quantities of unstructured sensor data and the military’s need to make sense of it also produces processing challenges that 5G could likely handle.

“5G offers faster download speeds, lower latency, and more capacity and connectivity for millions of devices and the possibilities for massive innovation,” says Lance Spencer, client executive vice president for defense, AT&T Public Sector and FirstNet (Oakton, Virginia). “5G’s ultra-low latency means faster response times when moving data like video and AR/VR [augmented reality/virtual reality] for immersive experiences. Its high reliability makes it ideal for supporting mission-­critical applications and services. Its massive connectivity capabilities enable faster aggregation of network-connected endpoints, sensors, devices, and data to power IoT connectivity.”

The all-encompassing nature of 5G is precisely what makes it such an attractive solution for the military. In areas where past network generations have had to go it alone, 5G and its proponents claim that few systems, waveforms, and data links would go unsupported under a 5G architecture.

“When people talk about 5G, a lot of times they think about the waveform that the cell carriers are bringing to market,” says Craig Miller, president of Viasat Government Systems (Carlsbad, California). “And yes, that is part of a 5G. It is a specific waveform in a way that radios communicate with each other, but the 5G standard and the set of 5G standards are much more than that. And I think that’s one of the things that sets 5G apart from 4G – the extensibility to create a 5G network-management infrastructure that can use additional waveforms.”

It’s notable that a network designed to be as impartial as 5G could actually be pivotal in multidomain operations and the act of bringing disparate systems together for the military. The added benefit of doing so under a simplified network-management system is something that 5G could excel at in comparison to 4G LTE. This would mean true interoperability under 5G for the DoD.

5G and how the military interoperates

“There’s sort of a historical precedent for this,” Miller says. “If you look at how successful interoperability has been achieved in the past, it’s usually by doing it at the ­network level or sometimes the application level. But the internet is an example of doing it at the network level where you have a TCP/IP (internet protocol suite) network and a bunch of different networks that aren’t even always compatible. But you do have the networking standards that allow them to interoperate through either the management or the gateway functions, and 5G can do this. It’s really a way that you can [capture] these disparate networks – those that would have been stovepiped in the past – and then use a 5G network-management architecture to bring them together.”

An important DoD program powered by the modern-day need for cross-domain solutions in the military is JADC2: The robust sensor connectivity that JADC2 was introduced to achieve could be successful under the implementation of a widely compatible 5G-powered network.

“Joint All-Domain Command and Control is key to enabling multi-domain operations,” AT&T/FirstNet’s Spencer says. “JADC2 and global operations, including space-based 5G terrestrial networks, will require the elimination of silos to ensure seamless communications between nodes. For the military, 5G technologies allow for the operation of several potential applications to include C2 [command and control], logistics, maintenance, training, AI [artificial intelligence], augmented and virtual reality, and ISR systems – all of which can benefit from improved data speeds and lower latency.”

Fielding a network as extensible, indiscriminate, and interoperable as 5G, however, will present security concerns, especially in multidomain defense arenas. Officials claim that the security question will influence how 5G networks and 5G network management systems are architected.

“As you bring more users together, there are more paths to give to any individual user. Being able to understand the data and metadata on your network and create a cyberdefense around that is one thing we’ve put a lot of time and energy into in the past decade,” Miller says. “This will be really important on 5G networks, especially in the JADC2 construct as you bring these networks together because you’re going to have to move beyond cyber hygiene and checklist-based and boundary-based cyberdefense and instead move to behavioral analysis and watching how users interact.”

Designing these security and signals-intelligence capabilities into 5G-powered architectures will also be an important part of the role 5G will play in EW theaters. The reason: While the 5G waveform isn’t specifically designed to work in contested environments, its scalability makes it ideal for congested spots.

Electronic warfare and 5G

Officials are excited about the possibility of 5G network-management systems designed to support various protected waveforms and thought to be ideal for EW environments. Pairing a native 5G network with supported waveforms that are built for low probability of detection could enable warfighters to roam between available networks, depending on the mission (Figure 1).

[Figure 1 omitted]

“The part of the 5G spec and waveform that’s operating in the millimeter band – those very high frequencies that tend to not propagate as far – create some capabilities that are a little more interesting in terms of the EW environment,” Miller says. “This is because it’s harder for the adversary to see them, simply because they don’t propagate as far. So, these little bubbles of operation are more difficult for adversaries to reach into. And a hybrid networking case where you have a 5G network with different physical layer waveforms, that also gives you room to play in an EW environment.”

Moreover, 5G could also fare well in EW arenas because it’s designed with the inherent ability to listen only to what it needs to, avoiding disruption from both accidental and purposeful signals that may get in the way. Even so, in the instance that disruption on the electromagnetic spectrum did occur, corresponding 5G-powered technologies could aid in identifying it.

“If an adversary is using 5G technology in the area, then EW systems will need to be able to understand if there’s 5G communication because this technology is not just owned by the U.S.,” Cowles says. “It’s worldwide, so adversaries could very well use 5G to communicate as well. EW systems will need to start being engineered to identify 5G signals and understand what adversaries could potentially be trying to communicate. That’s one side of it, and the other would be the fact that we use 5G technology and we don’t want unwelcome users to be able to disrupt or see what we’re doing. That’s where EW and 5G technology environments will have to coexist.”

Data collection and interpretation are so important to EW and are major pieces of the advantage 5G could provide on the battlefield. With the seemingly insurmountable quantities of data brought in by both military and commercial sensors, 5G-powered computing could better enable processing capabilities.

“5G allows for multiaccess edge computing (MEC), where data is processed locally near a device to speed the completion of computing tasks,” Spencer says. “MEC allows users to aggregate mission-critical data on site and offers the flexibility of delivering cloud services closer to the edge with localized compute functionality and optimized 5G cloud services. 5G networks are designed with robust, integrated cybersecurity protections to help secure user data.”

While edge computing is undoubtedly a start when it comes to military data analysis, there is still far too much of it for humans alone to process. Whether it’s anomalous network behavior, signals on the spectrum, or information from the cloud, automated 5G network-­management systems powered by AI could be pivotal in rendering out actionable details.

Pairing 5G with AI

“5G technologies could also be incorporated into ISR systems,” Spencer says. “These require increasingly high bandwidth to process, exploit, and disseminate intelligence data from a network of terrestrial and airborne sensors. This could enhance C2 by providing commanders with timely access to key intelligence and actionable information that can improve decision making in split seconds and allow commanders a better understanding of an adversary’s decision cycle.” (Figure 2.)

[Figure 2 omitted]

The faster and more efficient transmission of data that 5G could enable would thereby allow AI-powered analysis engines to run more effectively. Because AI and machine learning (ML) algorithms must be trained, enhanced low-latency access to data could result in smarter AI/ML systems.

“What 5G does bring is this somewhat open architecture where you can plug all kinds of different things in that could allow you to plug in different networks at the right level and offer the ability to command and control using the 5G network,” Cowles says. “Historically, with all of the different sensors and systems out there, it’s been very difficult to get actionable, multisensor data from all of the different deployed technologies to give you a cohesive, one-point location for that information. 5G makes that more likely because it can plug into different systems, assuming the necessary security is there.”

The evidence is stacking up: 5G is a network that is not only supportive of high data-throughput systems like that of AI/ML, but it also enables the maximization of such capabilities all the same. Apparent in the excitement surrounding 5G’s implementation is the evidence that players in the network-communications realm appear to be that much closer to tackling the big data problem faced by the military.

“We’ve only seen the tip of the iceberg in terms of what 5G can do,” Cowles says. “5G has such enormous potential and there are so many layers to it we haven’t even seen unlocked yet, and we’ll continue to see that AI will have a bigger role as 5G reaches its full potential.”

#### 5G cybersecurity ensures both effective use of hypersonic missiles and defense against hypersonic missiles.

Milo Medin 19, member of the Defense Innovation Board at the Department of Defense, Vice President of Access Services at Google; and Gilman Louie, expert and Special Government Employee to the Defense Innovation Board at the DoD, April 2019, “The 5G Ecosystem: Risks & Opportunities for DoD,” *Defense Innovation Board*, <https://apps.dtic.mil/sti/citations/AD1074509>, RMax

5G Impact on DoD

While much of the discussion around 5G revolves around the commercial sector as the driving force behind its rollout, 5G ecosystems of technology can equally revolutionize DoD operations, networks, and information processes. DoD must be able to communicate, engage, and operate faster to keep up with the changing environment. 5G will enable this new concept of operations, allowing larger volumes of data to be shared in close to real time across geographically dispersed systems. Currently, data sharing at that scale cannot be completed effectively with legacy communication networks. Existing networks will benefit by leveraging lower latency and higher capacity data transfer capability, but 5G’s true potential will be in its impact on the battle network of the future. That network will increasingly include a large number of cheaper, more connected, and more resilient systems to function in a rapidly evolving battlefield.

5G has the capability to combine DoD’s current fragmented networks into a single network to promote improved situational awareness and decision-making. This expanded reach will enable new technologies like hypersonic weapons and hypersonic defenses to be deployed, and has the potential to strengthen existing missions like nuclear C3. At an enterprise level, 5G can vastly improve day-to-day tasks such as logistics and maintenance, elevating the efficiency and speed of work across DoD.

However, 5G also presents a serious potential risk for DoD going forward. When operating overseas in the future, the vast majority of these networks and systems may depend on 5G infrastructure. If China leads the field in 5G infrastructure and systems, then the future 5G ecosystem will likely have Chinese components embedded throughout. This would pose a serious threat to the security of DoD operations and networks going forward. Additionally, the growth in the number of connected devices increases the potential “attack surface” for adversaries to target across DoD networks, which will require increased vigilance and security across systems. The larger volume of data being transferred will complicate this task, as it will make it more difficult to detect malicious traffic on a network.

#### Adversarial hypersonic weapons destroy early-warning capabilities---collapses nuclear deterrence.

William Schneider 22, senior fellow at the Hudson Institute, former under-secretary of state and chair of the Pentagon’s Defense Science Board, 2/6/2022, "China and Russia’s hypersonic weaponry threatens US early warning system," <https://www.ft.com/content/7d566088-7d25-4fde-9b02-311f86eb845e>, RMax

For those paying attention to the worrying advances in hypersonic weaponry by China and Russia, the news that the Pentagon is pushing US defence companies to hasten their own progress on hypersonic weapons is a welcome development. The race must now be on to catch up, or risk ceding the advantage to America’s adversaries.

Both China and Russia conducted hypersonic missile tests in the summer of 2021. Russia’s test of its hypersonic Skyfall nuclear-powered and nuclear-armed cruise missile took place at its Novaya Zemlya Island test range in the Arctic Ocean. Being nuclear powered, the missile has unlimited range.

China also conducted two flight tests of hypersonic ballistic missiles. One flew in a fractional earth orbit on a manoeuvring trajectory to the target region in China. The other also flew on a manoeuvring trajectory, and additionally released a second hypersonic object — a “first” for any nation.

The significance of these tests was quickly brushed off by both the arms control community and the media. Russia’s was reduced to environmental disregard (“a flying Chernobyl”) while China’s was dismissed as “nothing new” since Russian fractional orbital flights had taken placed during the cold war.

These reactions missed the importance of such capabilities in the nuclear modernisation efforts of both China and Russia. Manoeuvring hypersonic vehicles are not simply another means of delivering a nuclear warhead to a target. Instead, they are an essential part of a “system of systems” designed to defeat the US’s early warning abilities.

The US ballistic missile early warning system is a set of satellites and radars that are integrated with their command, control and communications system to detect, locate and track adversary missile attacks. Taken together, these interdependent capabilities are crucial to maintaining an effective nuclear deterrent. They were so fundamental to mutual deterrence during the cold war that the 1972 Anti-Ballistic Missile Treaty included provisions aimed at protecting them from attack.

The evolving importance of space has been obscured by the seamless way in which space capabilities have become integral to both everyday public life and national security. But operations there are decisive for nuclear deterrence.

Both China and Russia have well developed advanced offensive capabilities in space. In late January, for example, China’s Shijian 21 (CJ-21) satellite disappeared from its regular position in geostationary orbit 22,000 miles above the earth. The CJ-21 manoeuvred close to one of China’s malfunctioning satellites in its 35-satellite Beidou constellation. There it used a grappling arm to move the malfunctioning satellite to a “graveyard” orbit.

The Space Priorities Framework published by the Biden administration in December recognises space as “critical to modern warfare”, but continues to adhere to its position that the US will not use space for offensive military applications. This leaves our deterrent vulnerable to nations who do not share this view.

The US is developing a space-based system that uses advanced infrared sensors which may be able to detect manoeuvring hypersonic warheads. However, current missile defence systems do not permit them to engage with rapidly manoeuvring warheads. China and Russia have also developed counter systems that jeopardise US space monitoring and communications capabilities at low, medium and high altitudes.

By manoeuvring their satellites for offensive space operations adjacent to US satellites, China and Russia could conduct a wide variety of offensive operations. These include disrupting, spoofing or destroying sensors, on-board computation, data links or satellite electric power systems, and inserting malicious code using cyber techniques.

All of this is augmented by their ability to employ both cyber and kinetic capabilities to attack critical American infrastructure. This is the basis upon which military operations depend, as well as the electric power system, national telecommunications and the air and rail transportation systems that underpin US economic and military power.

China and Russia’s manoeuvring hypersonic missile capabilities enable these adversarial powers to have an integrated capacity to defeat the US early warning system. Under these circumstances, the US would be blind to an incoming foreign missile attack, and its ability to respond significantly constrained.

#### Hypersonic missiles ensure global war.

Richard Speier 17, Adjunct Staff with the RAND Corp, founded the Office of Non- Proliferation Policy at the DOD, received the Meritorious Civilian Service Medal for being the “father of the MTCR,” now consults in the Washington DC area; George Nacouzi, Senior Engineer at the RAND Corporation, supports projects within PAF (Project Air Force) and NSRD (National Security Research Division); Carrie A. Lee, researcher at RAND; Richard M. Moore, researcher at RAND, “Hypersonic Missile Nonproliferation: Hindering the Spread of a New Class of Weapons,” https://www.rand.org/pubs/research\_reports/RR2137.html

Strategic Implications of Hypersonic Weapons

Compressed Timelines

The U.S. military uses an acronym to describe the decisionmaking and action process cycle: OODA (Observe, Orient, Decide, Act). These four steps take time, and hypersonic missiles compress available response time to the point that a lesser nation’s strategic forces might be disarmed before acting. As an illustration of the time required to act with respect to an existential missile threat, the Nuclear Threat Initiative organization estimated a timeline for a U.S. response to a massive Russian intercontinental ballistic missile (ICBM) attack, as follows:9

• 0 minutes—Russia launches missiles

• 1 minute—U.S. satellite detects missiles

• 2 minutes—U.S. radar detects missiles

• 3 minutes—North American Aerospace Defense Command (NORAD) assesses information (2 minutes max)

• 4 minutes—NORAD alerts White House

• 5 minutes—first detonations of submarine-launched ballistic missiles

• 7 minutes—locate president and advisers, assemble them, brief them, get decision (8 minutes max)

• 13 minutes—decision

• 15 minutes—transmit orders to start launch sequence

• 20 minutes—launch officers receive, decode, and authenticate orders

• 23 minutes—complete launch sequence (2 minutes max)

• 25 minutes—Russian ICBM detonations.

This timeline is not, of course, representative of two hostile parties in closer proximity or with less effective warning systems than Russia and the United States. Nor is it representative of less-than-Armageddon possibilities. However, for adjacent enemies within a 1,000-km range, a hypersonic missile traveling at ten times the speed of sound could cover that distance and reduce response times to about six minutes.10

Targets

As discussed earlier, hypersonic missiles increase the threat over current generations of missiles in cases where the target nation has missile defenses. The targets in such nations would primarily be high value and heavily defended. Prime targets could include destroying a nation’s leadership and command and control, referred to as “decapitation,” to prevent the target nation from responding with an effective follow-on attack. Other key targets could be carrier strike groups, with the objective of striking a key blow or pushing the naval formation further from the coast. And, because of their time sensitivity, strategic forces and storage facilities for weapons of mass destruction (WMDs) could warrant hypersonic attack.

Implications for Targeted Nations

Any government faced with the possibility that hypersonic missiles would be employed against it—particularly in a decapitating attack— would plan countermeasures, many of which could be destabilizing. For example, countermeasures could include devolution of strategic forces’ command and control so that lower levels of authority could execute a strategic strike, which would obviously increase the risk of accidental strategic war; or strategic forces could be more widely dispersed— a tactic risking greater exposure to subnational capture. An obvious measure would be a launch-on-warning posture—a hair-trigger tactic that would increase crisis instability. Or the target nation could adopt a policy of preemption during a crisis—guaranteeing highly destructive military action. To be sure, such measures could be invoked against threats from current types of missiles.11 But, for nations with effective ballistic mis- sile and/or cruise missile defenses in the time frame when hypersonic missiles might proliferate, the hard choices would be forced when facing hypersonic threats.

Advanced nations with adequate resources could take other steps against hypersonic threats. They could strengthen the resilience of their command and control, harden the siting of their strategic forces, and make a deterrent force mobile or sea-based. These tactics may or may not be effective, especially for lesser nations. And they certainly will be expensive—putting them out of reach of some. Even for major powers, the proliferation of hypersonic missiles will create new threats by allowing lesser powers to hold them at risk of effective missile attacks especially against “unhardened” targets, e.g., cities. Over the coming decades, the ability of a lesser nation with a handful of ICBMs to threaten major powers will continue to decrease as wide area missile defenses continue to improve. However, HGVs and HCMs will be more difficult to defend against.

Implications for Major Powers

The ability of hypersonic missiles to penetrate advanced missile defenses will increase the risks for nations with such defenses. Lesser powers with hypersonic weapons may see these weapons as a deterrent against greater power intervention, and feel free to pursue potentially destabilizing regional agendas. Moreover, lesser nations with hypersonic missiles could affect the force deployments of major powers. As noted above, carrier strike groups might be pushed further out to sea or an intervening power’s regional military bases might become exposed to more effective attacks.

The Broader Picture of Increased Risk

The ability of hypersonic forces to penetrate defenses and compress decision time could aggravate the instabilities in regions that are already tense—for example, Iran-Israel and North Korea–Japan. Conflicts in these regions could evolve to include major powers aligned on opposite sides. An Israel-Iran conflict, with the United States and much of Europe aligned with Israel and Russia and perhaps China aligned with Iran, would create new paths for escalation to an even-larger conflict. The basic roles of external actors would not necessarily change—the alignments would stay the same—but external powers might suddenly find themselves in a more-unstable situation in which their patron states are increasingly trigger-happy. As noted previously, lesser powers could gain influence over major powers by threatening a hypersonic attack. At the least, lesser powers might be emboldened if they saw themselves as possessing a deterrent against major power intervention. Finally, because hypersonic weapons increase the expectation of a disarming attack, they lower the threshold for military action.

#### Secure 5G networks are key NATO operations:

#### 1---Air Power.

Fotios Kanellos 20, Cyberspace Subject Matter Expert at the Joint Air Power Competence Centre, inspection engineer for T-2 C/E aircraft and system engineer for the T-6A Flight Simulator at the Hellenic Air Training Command in Kalamata, June 2020, "Implications of 5G to Air Power – A Cybersecurity Perspective," *Joint Air & Space Power Conference*, <https://www.japcc.org/essays/implications-of-5g-to-air-power-a-cybersecurity-perspective/>, RMax

Cyber Threats

However, from a cyber-space perspective, 5G technology also increases drastically the attack surface (in some ways previously non-existent) and the number of potential entry points for attackers. The increased speed of the connected devices could make them more vulnerable to Distributed Denial-of-Service (DDoS) attacks. In today’s era of 4G/LTE mobile Internet, a large botnet10 formed simply by hacking a user’s home devices could be used to launch large-scale DDoS attacks against websites; in tomorrow’s b 5G network era, a similar botnet could disrupt an entire network of autonomous cars in a city11. As a result, the wide range of services and applications, as well as the novel features in the architecture, will introduce a plethora of new security challenges.

It was in September 2016 when hackers succeeded in scanning and exploiting hundreds of thousands of low-cost and low-powered IoT devices such as IP cameras, home routers, and digital video recorders, and turned them into remotely controlled bots by using ‘Mirai’ malware to launch large scale DDoS attacks. Not only 5G technology itself but also the communication between devices connected to the internet can be the weakest link in 5G’s security. If the manufactures of those low-cost interconnected devices do not embed cybersecurity standards in their products, the security risks will remain high.

5G networks and smart devices must adopt reliable and long-term security requirements beginning in the early stages of the design and manufacturing processes in order to fulfil their technological promises. By embracing a structured ‘cyber hygiene policy’, 5G technology can eventually be effectively implemented in Air Operations to improve communications and situational awareness.

Enhancing Air Power

NATO Allied Forces can gain great advantages by leveraging the novel features of 5G cellular technology. Communications and network operations in the air battlespace will be able to handle far more data at much faster speeds supporting real-time video streaming and VR applications. The wide employment of Unmanned Aerial Vehicles (UAVs) for purposes ranging from Intelligence, Surveillance & Reconnaissance (ISR) to airstrikes is expected to evolve even further in terms of geographic coverage and efficiency. Even logistic and maintenance activities, such as tracking maintenance stocks and conducting technical inspections, could benefit from a reliable and secure mobile connectivity.

Modern logistics systems such as the Autonomic Logistics Information System (ALIS) for the Joint Strike Fighter, are integrated with maintenance and operations procedures from across the world identifying problems with the aircraft, installing software updates, and providing preventive actions. 5G technology can clearly enhance productivity and safety of such complex, large-scale and interconnected military logistics operations transforming them to ‘sophisticated weapon systems’ ready to use even on the battlefield.

5G networks have the ability to expand the range of cloud-based applications and exponentially increase the amount of data transmitted and exchanged during air combat operations. The challenge of infobesity (information overload) can still be encountered using digital technologies that take advantage of the super-fast, high-bandwidth and low-latency communication environment that 5G provides. Consolidating the extracted information from internet-connected sensors and platforms, and immediately distributing the acquired knowledge to the Command and Control structure is essential to facilitate ‘smart’ decision-making12. Therefore, securing (allied) military networks and maintaining their high level of interoperability will become even more critical.

According to an ‘EU coordinated risk assessment report’13, published on 9 October 2019, among the main threats and vulnerabilities of 5G networks are the high dependencies on individual suppliers. The lack of diversity in equipment and infrastructure can lead to increased exposure to attacks by State-sponsored actors who interfere with the suppliers. Thus, the individual risk profile of suppliers will become particularly important, especially for those with significant presence within networks.

In order to develop a secure 5G mobile network strategy, the US Department of Defence (DoD) decided, about a year ago, to strengthen the requirements for the supply chain of innovative technology products, including subcontractors, by introducing higher cybersecurity standards that would ensure resiliency to cyber-attacks. The established public-private partnership, known as ‘Trusted Capital Marketplace’, connects defence technology start-ups with trusted sources of capital in order to secure the delivery of such critical emerging technologies14.

Future Challenges

With the future stand-alone 5G ecosystem, as described above, all network functionalities will be virtualised based on software rather than hardware, and take place within a single cloud environment. 5G networks are going to be deployed in a complex global cybersecurity threat landscape. To ensure confidentiality (authorised access), integrity (accurate information) and availability (any time access) with such a revolutionary technology and confront the challenges derived from it, NATO member and partner countries will have to follow a new security paradigm. Current cybersecurity models and policies must be reassessed and new security frameworks applied in order to mitigate risks and threats.

Are Alliance members determined to invest the resources necessary for establishing a resilient and secure infrastructure for 5G technology? Are we willing to adapt to this emerging technology at the speed of change and not lagging behind other competing nations? Those questions have to be answered as clearly and decisively as possible in the very near future.

#### 2---Naval Power.

Capela ’21 [Germano; July 2021; Radio Engineer at the NATO Communications and Information Agency, M.S. in Electrical and Computer Engineering from the Instituto Superior Técnico, M.Sc. in Electrical, Electronics, and Communications Engineering from Escola Naval; et al.; "5G for deployable and maritime communications," https://doi.org/10.1109/ICMCIS52405.2021.9486397]

In this section we propose an experiment, using the combined 5G proof-of-concept prototype, to assess the feasibility of 5G-enabled concepts for providing coastal communications in support of ship-shore and relayed ship-ship-shore communications, as depicted in the left portion of Fig. 1. In such conditions, ships are in line-of-sight (LOS) distances to shore based infrastructures and between each other (typically less than 20 km), in a benign/friendly territory and far from intentionally contested EM environment. For this scenario, it is considered the use of high-performance 5G systems to provide interoperable, high capacity, extended coverage and low latency connectivity between commands ashore and afloat.

B. Technical Concept

In this context, a primarily PTMP shore based system enables high throughput reach back communications for ships that are within coastal coverage. This allows non satellite communications (SATCOM) capable units to effectively reach back and access C2 and enterprise systems, while at sea. This solution also provides a backup medium against SATCOM downtimes, or even an offloading route to SATCOM traffic, within the areas mentioned. Considering a naval force scenario in the areas mentioned, a combination of PTMP and mesh topologies can effectively extend the limits of LOS coverage by shore based systems, through multi–hop range extension. Maritime scenarios typically address multinational operations, therefore interoperability between systems is key for effective communications between different nations.

Even though most ships these days are fitted with SATCOM reach back systems, such systems might not necessarily be used/available for all the range of assigned missions, due to availability and cost reasons. SATCOM is costly to operate, both on–board and on the ground/space segments, which might not be necessary in mainly shallow water operations. Alternatively, HF based beyond line of sight (BLOS) reach back systems are utilized, but with very limited throughput capacity, offering a very last resort alternative to SATCOM reach back services. For ships operating in close proximity (i.e. within LOS), ship-ship communications based on SATCOM are very inefficient, as the delay and jitter introduced by each reach back link significantly impact real time dissemination of information.

Currently, NATO does not use these concepts, as traditional enabling LOS radio technologies (e.g. V/UHF tactical radios) do not offer suitable performance to be used as alternative to SATCOM. On the other hand, traditional IMT technologies, such as LTE, have limited spectrum supportability and limited antenna technology to handle interference, challenging propagation and environmental conditions (e.g. ships mobility and dynamics (roll and pitch) limit the use of stationary high gain antennas).

The likelihood and severity of EW threats in coastal communications is deemed low, as this scenario consists of ships operating in NATO territory, in benign/friendly areas and far from intentionally contested EM environments. Nevertheless, from a ship’s perspective, the EM environment can be regarded as complex for two reasons:

Military vessels are complex compositions of radio– enabled systems, resulting in crowded and packed antenna farms, which potentiates mutual interference phenomena.

As ships approach coastal areas, the exposure to various sources of (unintentional) interference increases dramatically as a result of land–based systems radiating towards the sea.

Deploying ship-shore and ship-ship communications based on 5G technology (which has intrinsic frequency and antenna agility features) would provide significant operational benefits, such as:

* Effective alternative to SATCOM reach back links in coastal areas.
* Multinational interoperability based on international standards.
* Multi–hop range extension for groups of ships operating in close proximity.
* Low latency and high throughput ship-ship communications.

C. Requirements for a 5G–based Proof of Concept

As this scenario concerns the use of shore-based infrastructures in benign/friendly territory, the backbone of the 5G-based concept, i.e. the 5G core and radio access network, can be based on either publicly or privately owned infrastructure. The selected approach will significantly depend on the requirements of the target implementations, namely, coverage, operation and management models and security. The proposed technical architecture is illustrated in Fig. 3.

For this architecture, a two-tier high-capacity 5G-based system, with multiband support, i.e. support to the 700 MHz (low band) and the 5G Sub–6–GHz (ideally in the 4.4-5.0 GHz NATO Band IV) frequency bands, would provide both capacity and flexibility in various link and EM conditions. Multiband support and frequency agility are vital strategies for adequate coexistence in complex EM environment, i.e. coexistence with other radio and sensor systems and exposure to shore-based interferences, and for dynamic adaptation to varying propagation conditions. For the use of public networks, network slicing is identified as enabler of services and network segregation (control and user planes), but it also becomes a relevant security feature for military use of public infrastructure due to its network segregation properties.

#### Air and naval power deter rogue states and WMD proliferation.

Michael Johnson 14 & Terrence K. Kelly. Michael Johnson is a Senior Defense Research Analyst at the RAND Corporation. Dr. Terrence K. Kelly is Director of the Strategy, Doctrine, and Resources Program at the RAND Arroyo Center. 3rd Quarter 2014. “Tailored Deterrence: Strategic Context to Guide Joint Force 2020.” https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-74/jfq-74\_22-29\_Johnson-Kelly.pdf

There is little historical evidence that air and naval power alone is sufficient, but much to suggest that a unified joint force can deter and defeat aggression quite effectively. Since Giulio Douhet first theorized that airpower could win wars by itself by terrorizing a population and causing a government to capitulate (that is, “shock and awe”), these theories have repeatedly failed, been updated, and again proved wanting. Strategic bombing failed to defeat aggression by Germany and Japan, but air superiority enabled decisive joint offensives to defeat their military forces. While Operation Linebacker had greater coercive effect than Rolling Thunder, the Vietnam War would not have ended without integrated air-land operations that defeated the 1972 North Vietnamese offensive on the ground. In Desert Storm, air operations failed to force Iraq to withdraw from Kuwait, but degraded the enemy and helped ground forces achieve campaign objectives in 100 hours with 148 U.S. battle deaths. In Kosovo, airstrikes were a critical component of a successful coercion campaign, but they were insufficient to compel Slobodan Miloševic´ to halt ethnic cleansing or agree to terms without the credible threat of ground operations.27 In Afghanistan, strategic air attacks failed to defeat the Taliban, but precision close air support enabled Afghan allies with U.S. special operations forces to seize Mazar-e-Sharif and Kabul. In Iraq, airstrikes failed to “shock and awe” Saddam Hussein and his security forces into surrender, but they enabled and protected dispersed small units operating over wide areas.

Thus the leaders of North Korea, Iran, and Syria may well conclude that sanctions and airstrikes alone are not sufficient to deter them from attacking neighbors, killing civilians, launching catastrophic cyber attacks, or supporting terrorist attacks against the homeland. If adversaries believe they can achieve their objectives by exploiting irregular tactics or complex terrain, then the threat of airstrikes may not “deter by denial.” If adversaries believe the cost of agreeing to U.S. terms is unacceptable and remain willing to endure hardships, then the threat of airstrikes may not “deter by punishment” or compel them to concede. The United States typically demands a significant sacrifice from an adversary without considering his reaction—for example, a dictator must abdicate (for example, Libya and Syria) or relinquish an important territory (Kuwait and Kosovo). In cases in which a leader’s survival depends on his or her demonstrated power to rule, resistance may well be preferable to surrender.

If the optimistic force-sizing assumptions about the efficacy of smart power prove invalid in future contingencies, there would be significant military risk to defeat aggression and respond to another contingency, and higher risk if continued budget cuts reduce Active-duty end-strength well below currently programmed levels or compromise readiness. This means that combatant commanders would lack the forces required to achieve strategic objectives, or Reserve forces would be deployed in combat before they are fully trained, or land forces would remain in direct combat much longer than evidence suggests could be reasonably endured by volunteer citizens without compromising the quality of the force.28

The alternative approach to deterring and defeating regional aggression would restore emphasis on decisive joint campaigns within the force-planning construct while still including other missions such as irregular warfare, counterterrorism, peacekeeping, and homeland defense. Specifically, Joint Force 2020 would be sized to conduct operations as joint campaigns that stress all Services in terms of critical capabilities (see table).

[[TABLE OMITTED]]

The force-planning construct shown in the table offers advantages that enhance regional deterrence. In cases of conflict with North Korea and Syria, ground forces enable the joint force to:

protect people, defend territory, and secure resources

defeat threats in complex terrain

achieve a favorable and longer lasting outcome

demonstrate U.S. resolve to allies and adversaries.

These advantages are relevant in deterring the emergent challenges defined above. For example, to deter nuclear transfer and terrorism,

*target states should announce they reserve the right to take large-scale military action, to include invasion and occupation, against territories of central importance to any non-state actor that attacks them with nuclear weapons, and any entity that provides the attackers with substantial material or financial support.29*

This decisive joint capability would introduce uncertainty into adversary calculations, as well as the calculations of their hosts and supporters should they be nonstate actors and cause them to consider the consequences of their actions beyond enduring airstrikes.

The result of this alternative approach is a balanced joint force with the credible capability to deter and defeat aggression by rogue states, secure WMD in failing states, and still deter China from attacking U.S. allies. It provides the President with more flexible options to respond to unforeseen events. The disadvantage for some defense planners is that disproportionate cuts to ground forces were intended to pay for offensive Air-Sea Battle capabilities to defeat China in a war for which there is no credible theory for victory, and given the risk of mutual economic or nuclear destruction, one that no President or Secretary of Defense would willingly enter.

#### Independently, 5G cybersecurity prevents NC3 entanglement.

Robert Spalding 22, former Senior Director of Strategy to the President at the National Security Council, founder and CEO of SEMPRE, retired Air Force Brigadier General, 6/30/2022, "Viewpoint: JADC2 Should Embrace Hardened 5G, Edge Computing," https://www.nationaldefensemagazine.org/articles/2022/6/30/jadc2-should-embrace-hardened-5g-edge-computing, RMax

Joint all-domain command and control, or JADC2, is the military’s latest buzzy acronym and one of the stated priorities for the Defense Department. Yet it is a concept without a clear solution and is likely to languish without the infrastructure to ensure its success.

One of the biggest challenges for JADC2 is interoperability. Today, just in nuclear command and control, which is a subset of JADC2, there are more than 100 programs underway. Since these programs often involve technology that was not built to be interoperable, bridging information is a challenge. Data becomes trapped and unable to be used quickly to build a comprehensive picture for decision makers.

The question becomes, why not use the cloud? There, the focus is on data transport. If we could just get the data to the cloud, then we could solve many of the problems. But then that raises the question, which cloud? And inevitably, how do I move my data there?

There are many different clouds with different architectures, which makes managing information across disparate platforms difficult. And there is no easy way to onboard cloud service providers. The department attempted to do so through a competition called the Joint Enterprise Defense Infrastructure initiative. Doomed from the start, the program envisioned a winner-take-all cloud service procurement scenario. If that is not a recipe for stagnant innovation, I’m not sure what is.

So, how does the military move data? There are numerous transport networks that are designed to carry the bits and bytes of JADC2 back to some all-knowing cloud — Starlink, OneWeb, Hughes Network Systems, Lockheed Martin, Boeing, Iridium and on and on. Which will win?

Probably all in some fashion since the pie is so big. And that’s just the satellite providers. Don’t forget the telecom service providers and fiber-optic companies, which also play a part in this orchestra.

What is consistent about these technologies? They represent separate networks that need a gateway and a location to on-ramp and off-ramp data between and among them.

The answer the tech industry seems to be offering is the cloud. The cloud, however, is not ubiquitous. The data centers that can be the gateways for moving, transferring and processing data are often large and centralized. This presents an incredible juicy target for would-be attackers.

Even if they were one single network, we still wouldn’t have the bandwidth to move the bulk of the data to the cloud. Often, by the time data does make it to the cloud, it is too late to enable the processing required to make the information gleaned actionable. Once again, warfighters are stuck with data islands.

Multiple independent networks and stuck data turn out to be two main challenges that the Defense Department needs to solve. How is it possible to harness the power of the commercial sector to solve these problems? The answer lies in 5G and edge computing.

5G is best known for providing the radio access technology in the latest generation of cellular networks, but it is far more than that. 5G also represents the implementation of virtual network functions, software-defined networking and transport gateways for the already interoperable wireless networks.

The industry standards body, 3rd Generation Partnership Project, or 3GPP, has taken on this challenge. A recent release envisions a set of standards for interoperability that combines computers, networking and storage across the different layers of commercial communication. It covers radio-access network standards to include network-to-network links. Properly configured, a 5G stand-alone network anywhere in the world should be able to hand off a slice of the network to a device according to the resource needs of the customer.

At the heart of 5G is edge computing. Without edge computing, trapped data will become a problem for commercial cellular networks as the devices attached to 5G networks multiply with their use.

Autonomous systems and the artificial intelligence algorithms that seek to make sense of data at the edge will require computing at the edge.

There will not be enough bandwidth to transport the data to centralized clouds for processing. These edge nodes will bring the power of applications to the data. Some of these applications will create the opportunity for wireless gateways at the edge that bring fiber, telecom and satellite together into one seamless network. This network can be reconfigured on the fly, for any application, because it is entirely constructed in software.

It seems logical that embracing commercial 5G and edge computing standards for JADC2 would be a no-brainer. The problem is that 3GPP is not built for the battlefield.

Commercial networks are built to commercial standards. As a former B-2 pilot, commercial networks look like an easy target, and judging from the bombing two years ago of a Nashville AT&T communications hub, you don’t even need a plane to take them down.

How do you build a 21st century secure, hardened, hyper-converged network? First, it would be electromagnetic pulse hardened. Russia, China and North Korea — and soon perhaps Iran — have nuclear weapons. Depending on the altitude of the burst, a single nuclear weapon detonated in the upper atmosphere above the United States could take out the grid and communications networks and data centers.

Second, the network would be resistant to physical tampering and ensure the provenance and security of both the hardware and software.

Third, the personnel who work on this network would be vetted, and more than one would be required to do any work of a critical nature on the hardware or software.

Finally, the network would be configured in such a way so that classified systems could operate securely on the infrastructure, alongside commercial applications.

#### NC3 entanglement guarantees escalation---maintaining stable communications is key.

Michael Klare 19, professor emeritus of peace and world security studies at Hampshire College, November 2019, “Cyber Battles, Nuclear Outcomes? Dangerous New Pathways to Escalation,” *Arms Control Association*, <https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation>, edited for ableist language

In January 2018, details of the Trump administration’s Nuclear Posture Review (NPR) were posted online by the Huffington Post, provoking widespread alarm over what were viewed as dangerous shifts in U.S. nuclear policy. Arousing most concern was a call for the acquisition of several types of low-yield nuclear weapons, a proposal viewed by many analysts as increasing the risk of nuclear weapons use.

Another initiative incorporated in the strategy document also aroused concern: the claim that an enemy cyberattack on U.S. nuclear command, control, and communications (NC3) facilities would constitute a “non-nuclear strategic attack” of sufficient magnitude to justify the use of nuclear weapons in response.

Under the Obama administration’s NPR report, released in April 2010, the circumstances under which the United States would consider responding to non-nuclear attacks with nuclear weapons were said to be few. “The United States will continue to…reduce the role of nuclear weapons in deterring non-nuclear attacks,” the report stated. Although little was said about what sort of non-nuclear attacks might be deemed severe enough to justify a nuclear response, cyberstrikes were not identified as one of these. The 2018 NPR report, however, portrayed a very different environment, one in which nuclear combat is seen as increasingly possible and in which non-nuclear strategic threats, especially in cyberspace, were viewed as sufficiently menacing to justify a nuclear response. Speaking of Russian technological progress, for example, the draft version of the Trump administration’s NPR report stated, “To…correct any Russian misperceptions of advantage, the president will have an expanding range of limited and graduated [nuclear] options to credibly deter Russian nuclear or non-nuclear strategic attacks, which could now include attacks against U.S. NC3, in space and cyberspace.”1

The notion that a cyberattack on U.S. digital systems, even those used for nuclear weapons, would constitute sufficient grounds to launch a nuclear attack was seen by many observers as a dangerous shift in policy, greatly increasing the risk of accidental or inadvertent nuclear escalation in a crisis. “The entire broadening of the landscape for nuclear deterrence is a very fundamental step in the wrong direction,” said former Secretary of Energy Ernest Moniz. “I think the idea of nuclear deterrence of cyberattacks, broadly, certainly does not make any sense.”2

Despite such admonitions, the Pentagon reaffirmed its views on the links between cyberattacks and nuclear weapons use when it released the final version of the NPR report in February 2018. The official text now states that the president must possess a spectrum of nuclear weapons with which to respond to “attacks against U.S. NC3,” and it identifies cyberattacks as one form of non-nuclear strategic warfare that could trigger a nuclear response.

That cyberwarfare had risen to this level of threat, the 2018 NPR report indicated, was a product of the enhanced cybercapabilities of potential adversaries and of the creeping obsolescence of many existing U.S. NC3 systems. To overcome these vulnerabilities, it called for substantial investment in an upgraded NC3 infrastructure. Not mentioned, however, were extensive U.S. efforts to employ cybertools to infiltrate and potentially incapacitate the NC3 systems of likely adversaries, including Russia, China, and North Korea.

For the past several years, the U.S. Department of Defense has been exploring how it could employ its own very robust cyberattack capabilities to compromise or destroy enemy missiles from such states as North Korea before they can be fired, a strategy sometimes called “left of launch.”3 Russia and China can assume, on this basis, that their own launch facilities are being probed for such vulnerabilities, presumably leading them to adopt escalatory policies such as those espoused in the 2018 NPR report. Wherever one looks, therefore, the links between cyberwar and nuclear war are growing.

The Nuclear-Cyber Connection

These links exist because the NC3 systems of the United States and other nuclear-armed states are heavily dependent on computers and other digital processors for virtually every aspect of their operation and because those systems are highly vulnerable to cyberattack. Every nuclear force is composed, most basically, of weapons, early-warning radars, launch facilities, and the top officials, usually presidents or prime ministers, empowered to initiate a nuclear exchange. Connecting them all, however, is an extended network of communications and data-processing systems, all reliant on cyberspace. Warning systems, ground- and space-based, must constantly watch for and analyze possible enemy missile launches. Data on actual threats must rapidly be communicated to decision-makers, who must then weigh possible responses and communicate chosen outcomes to launch facilities, which in turn must provide attack vectors to delivery systems. All of this involves operations in cyberspace, and it is in this domain that great power rivals seek vulnerabilities to exploit in a constant struggle for advantage.

The use of cyberspace to gain an advantage over adversaries takes many forms and is not always aimed at nuclear systems. China has been accused of engaging in widespread cyberespionage to steal technical secrets from U.S. firms for economic and military advantages. Russia has been accused, most extensively in the Robert Mueller report, of exploiting cyberspace to interfere in the 2016 U.S. presidential election. Nonstate actors, including terrorist groups such as al Qaeda and the Islamic State group, have used the internet for recruiting combatants and spreading fear. Criminal groups, including some thought to be allied with state actors, such as North Korea, have used cyberspace to extort money from banks, municipalities, and individuals.4 Attacks such as these occupy most of the time and attention of civilian and military cybersecurity organizations that attempt to thwart such attacks. Yet for those who worry about strategic stability and the risks of nuclear escalation, it is the threat of cyberattacks on NC3 systems that provokes the greatest concern.

This concern stems from the fact that, despite the immense effort devoted to protecting NC3 systems from cyberattack, no enterprise that relies so extensively on computers and cyberspace can be made 100 percent invulnerable to attack. This is so because such systems employ many devices and operating systems of various origins and vintages, most incorporating numerous software updates and “patches” over time, offering multiple vectors for attack. Electronic components can also be modified by hostile actors during production, transit, or insertion; and the whole system itself is dependent to a considerable degree on the electrical grid, which itself is vulnerable to cyberattack and is far less protected. Experienced “cyberwarriors” of every major power have been working for years to probe for weaknesses in these systems and in many cases have devised cyberweapons, typically, malicious software (malware) and computer viruses, to exploit those weaknesses for military advantage.5

Although activity in cyberspace is much more difficult to detect and track than conventional military operations, enough information has become public to indicate that the major nuclear powers, notably China, Russia, and the United States, along with such secondary powers as Iran and North Korea, have established extensive cyberwarfare capabilities and engage in offensive cyberoperations on a regular basis, often aimed at critical military infrastructure. “Cyberspace is a contested environment where we are in constant contact with adversaries,” General Paul M. Nakasone, commander of the U.S. Cyber Command (Cybercom), told the Senate Armed Services Committee in February 2019. “We see near-peer competitors [China and Russia] conducting sustained campaigns below the level of armed conflict to erode American strength and gain strategic advantage.”

Although eager to speak of adversary threats to U.S. interests, Nakasone was noticeably but not surprisingly reluctant to say much about U.S. offensive operations in cyberspace. He acknowledged, however, that Cybercom took such action to disrupt possible Russian interference in the 2018 midterm elections. “We created a persistent presence in cyberspace to monitor adversary actions and crafted tools and tactics to frustrate their efforts,” he testified in February. According to press accounts, this included a cyberattack aimed at paralyzing the Internet Research Agency, a “troll farm” in St. Petersburg said to have been deeply involved in generating disruptive propaganda during the 2016 presidential elections.6

Other press investigations have disclosed two other offensive operations undertaken by the United States. One called “Olympic Games” was intended to disrupt Iran’s drive to increase its uranium-enrichment capacity by sabotaging the centrifuges used in the process by infecting them with the so-called Stuxnet virus. Another left of launch effort was intended to cause malfunctions in North Korean missile tests.7 Although not aimed at either of the U.S. principal nuclear adversaries, those two attacks demonstrated a willingness and capacity to conduct cyberattacks on the nuclear infrastructure of other states.

Efforts by strategic rivals of the United States to infiltrate and eventually degrade U.S. nuclear infrastructure are far less documented but thought to be no less prevalent. Russia, for example, is believed to have planted malware in the U.S. electrical utility grid, possibly with the intent of cutting off the flow of electricity to critical NC3 facilities in the event of a major crisis.8 Indeed, every major power, including the United States, is believed to have crafted cyberweapons aimed at critical NC3 components and to have implanted malware in enemy systems for potential use in some future confrontation.

Pathways to Escalation

Knowing that the NC3 systems of the major powers are constantly being probed for weaknesses and probably infested with malware designed to be activated in a crisis, what does this say about the risks of escalation from a nonkinetic battle, that is, one fought without traditional weaponry, to a kinetic one, at first using conventional weapons and then, potentially, nuclear ones? None of this can be predicted in advance, but those analysts who have studied the subject worry about the emergence of dangerous new pathways for escalation. Indeed, several such scenarios have been identified.9

The first and possibly most dangerous path to escalation would arise from the early use of cyberweapons in a great power crisis to paralyze [compromise] the vital command, control, and communications capabilities of an adversary, many of which serve nuclear and conventional forces. In the “fog of war” that would naturally ensue from such an encounter, the recipient of such an attack might fear more punishing follow-up kinetic attacks, possibly including the use of nuclear weapons, and, fearing the loss of its own arsenal, launch its weapons immediately. This might occur, for example, in a confrontation between NATO and Russian forces in east and central Europe or between U.S. and Chinese forces in the Asia-Pacific region.

Speaking of a possible confrontation in Europe, for example, James N. Miller Jr. and Richard Fontaine wrote that “both sides would have overwhelming incentives to go early with offensive cyber and counter-space capabilities to negate the other side’s military capabilities or advantages.” If these early attacks succeeded, “it could result in huge military and coercive advantage for the attacker.” This might induce the recipient of such attacks to back down, affording its rival a major victory at very low cost. Alternatively, however, the recipient might view the attacks on its critical command, control, and communications infrastructure as the prelude to a full-scale attack aimed at neutralizing its nuclear capabilities and choose to strike first. “It is worth considering,” Miller and Fontaine concluded, “how even a very limited attack or incident could set both sides on a slippery slope to rapid escalation.”10

What makes the insertion of latent malware in an adversary’s NC3 systems so dangerous is that it may not even need to be activated to increase the risk of nuclear escalation. If a nuclear-armed state comes to believe that its critical systems are infested with enemy malware, its leaders might not trust the information provided by its early-warning systems in a crisis and might misconstrue the nature of an enemy attack, leading them to overreact and possibly launch their nuclear weapons out of fear they are at risk of a preemptive strike.

“The uncertainty caused by the unique character of a cyber threat could jeopardize the credibility of the nuclear deterrent and undermine strategic stability in ways that advances in nuclear and conventional weapons do not,” Page O. Stoutland and Samantha Pitts-Kiefer wrote in 2018 paper for the Nuclear Threat Initiative. “[T]he introduction of a flaw or malicious code into nuclear weapons through the supply chain that compromises the effectiveness of those weapons could lead to a lack of confidence in the nuclear deterrent,” undermining strategic stability.11 Without confidence in the reliability of its nuclear weapons infrastructure, a nuclear-armed state may misinterpret confusing signals from its early-warning systems and, fearing the worst, launch its own nuclear weapons rather than lose them to an enemy’s first strike. This makes the scenario proffered in the 2018 NPR report, of a nuclear response to an enemy cyberattack, that much more alarming.

#### Coordinating NATO efforts closes interoperability gaps and fulfills 5G’s full potential in the military domain.

Lauren Speranza 21, director of the Transatlantic Defense and Security Program for the Center for European Policy Analysis; and Jack Crawford, researcher at the Transatlantic Defense and Security Program for the Center for European Policy Analysis, 7/8/2021, "Making 5G an Ally of the Euro-Atlantic Area," <https://cepa.org/making-5g-an-ally-of-the-euro-atlantic-area/>, RMax

The advent of 5G technology is heralded as the glue that will enable the integration of emerging and disruptive technologies (EDTs) into military operations.

NATO militaries are shifting from a platforms-based defense to one revolving around systems. This would see long-term, multipurpose assets like tanks and aircraft carriers replaced by narrowly purposed, nimble, expendable, and data-informed capabilities fully integrated into the force structure. But the effective collection, sharing, and operational potential of data in the decision-making process will only be possible if 5G networks are advanced and resilient.

There is a problem here — 5G’s capacity to revolutionize conflict is still somewhat unknown. Discrepancies between NATO allies in their approaches to 5G procurement and operational frameworks risk creating interoperability gaps in fulfilling its military potential. Nevertheless, some individual allies are beginning important national efforts that can serve as a basis for broader coordination around military 5G.

For example, Latvia’s progress in 5G military testing might serve as a basis for developing principles that NATO allies can use to strengthen the resilience and capacity of their military 5G networks. These include:

* prioritizing resilience through redundancy
* broadband-spectrum sharing
* enhancing interoperability, and
* industrial and regulatory collaboration.

In December, Latvia unveiled Europe’s first 5G military testing site at Ādaži Military Base, which allows Latvian and NATO forces to test, uncover and resolve security vulnerabilities in the network. This site enables deeper integration into defense systems and provides alliance members with “testing grounds” for innovative 5G applications. The Ādaži base can also offer lessons to other NATO members as they develop their national 5G capabilities for military use, including the possibilities of 5G in autonomous systems and Joint-All Domain Command and Control (JADC2), the U.S. program to connect all military and space sensors in a single network. Continued, joint testing is the most important way to refine the possibilities of 5G in future warfare characterized by autonomous systems, data, algorithms, and JADC2.

These advancements, however, pale in comparison to the 5G developments by adversarial states. China is a pioneer, having already developed 5G unmanned aerial vehicle (UAV) applications for package deliveries, aerial photographs, and emergency communications. Western states must develop their 5G defense capabilities strategically to remain competitive and make up for the lost time.

The dual-use functionality of 5G technology means that a broad range of actors including the military, security services, civil society, and private companies are integral to achieving resilience and effective implementation. Redundant structures and systems, especially between government and commercial enterprises, reduce the ability of malign actors to immobilize those systems by creating multiple networks for operation. This redundancy also integrates civil sector network defense, bolstering the potential for a whole-of-society response to threats.

There is some debate on how best to allocate the broadband spectrum between governments and civil society, which determines how insulated 5G defense systems are from attacks. For NATO defenses, dividing spectrum access between governments and civil society might prove to be more effective than allowing dual access to the same spectrum portions. NATO should take advantage of its prerogative as a multinational coordinating body to facilitate spectrum use standardization across the alliance.

Enhancing interoperability is perhaps the most important factor for 5G military application and will depend on alliance-wide standardization. As 5G allows for more connectivity and flexibility, as well as higher data volumes, it also enables greater dynamism and fluidity of information flows within defense systems. This can increase warning times, speed of decision-making, and response times in crisis and pre-crisis scenarios. The alliance should capitalize on this unprecedented potential for interconnectedness to increase resilience and expand the redundancy of systems.

Finally, national governments must leverage Western technology and regulatory diplomacy to create international standards for 5G technology to ensure its governance is not monopolized by adversaries. This would also go a long way to enhancing interoperability amongst allies and instilling network resilience at the heart of 5G development. The formalization of regulatory frameworks for 5G was recently emphasized in a UK House of Commons Science and Technology Committee report, which labeled it essential if NATO members hope to retain technological influence. Thus, international regulatory agreements will become increasingly important to ensure a democratic digital domain not dominated by autocratic powers.

Integrating these factors into 5G technology development better positions NATO to realize the potential of EDTs and to improve the resilience of these systems to disruption. This should be reflected in the short-term in NATO allies’ approach to building 5G digital backbones. The alliance also cannot lose sight of the risks associated with military 5G implementation. Not only are temporary measures needed to implement 5G technology securely, but Western allies must have the long-term strategic foresight to lead the way in the development of 6G and quantum technology, which will eventually replace 5G.

The recent NATO communique from the Brussels Summit promises meaningful contributions in this regard, via the civil-military Defense Innovation Accelerator and NATO Innovation Fund. Though it will be years before we can gauge the success of these measures, internal collaboration with industry experts across the private sector, as well as cross-border coordination with allies to outline governing and operational frameworks, will be essential.

### Plan---1AC

#### Plan: The United States federal government should substantially increase its security cooperation with the North Atlantic Treaty Organization for fifth-generation telecommunications cybersecurity.

#### Plan: The United States federal government should increase security cooperation with the North Atlantic Treaty Organization for fifth-generation telecommunications including at least cybersecurity standards, certification, and information-sharing.

### Solvency---1AC

#### Security cooperation with NATO solves security and leadership in 5G.

DaSilva ’20 [Luiz; December 2020; Bradley Professor of Cybersecurity and Executive Director Commonwealth Cyber Initiative at Virginia Technology, Ph.D. in Electrical Engineering from the University of Kansas; et al.; "Securing 5G: NATO’s Role in Collaborative Risk Assessment and Mitigation," <https://ccdcoe.org/uploads/2020/12/4-Securing-5G_ebook.pdf>]

5. RECOMMENDATIONS FOR NATO’S SUPPORT TO GLOBAL 5G SECURITY COOPERATION

A. International Partnership for Risk Assessment and Product Testing

Countries must conduct a risk assessment of their security processes and adopt advanced security measures to ensure the successful deployment of 5G. A consortium of NATO nations and its strategic partners working together to develop cyber risk management policies for 5G systems is paramount. For example, the EU toolbox for 5G security (NIS Cooperation Group, 2020) has provided member states with the opportunity to conduct a gap analysis and launch new initiatives to improve existing security measures and enforcement mechanisms. The toolbox has aided a systematic self-assessment and has resulted in several member states being prepared to adopt advanced security measures on 5G cyber security. This initiative should be expanded to and adopted by non-EU NATO nations.

NATO and the Allies must each develop a strategy to ensure security by design for 5G beyond infrastructure deployment. This should include a rigorous process for vetting vendors and carriers of such networks. This process should be laid out by an international consortium of industry and government stakeholders, including the NATO Standardization Office (NSO) and other entities such as relevant Centres for Excellence that would look at balancing risk mitigation and security. The consortium should explore approaches to establishing and maintaining situational awareness over 5G supply chains and security practices of suppliers and vendors. This organisation would ensure that 5G products comply with security specifications provided by the 3GPP and other key standardisation bodies. It should also develop a framework for assessment, mitigation and management of the range of risks to 5G networks. This includes developing testing tools for automated evaluation of the security of 5G networks; artificial intelligence solutions that rely on shared data are promising candidates for this. Finally, the consortium should incentivise improvements in security with initiatives such as (i) easy access to license-free or lightly-licensed spectrum to incentivise innovation: (ii) incentives for shared accountability in the supply chain that results in access to trustworthy hardware and software: and (iii) investigation of new business models that incentivise manufacturers and operators that meet security benchmarks.

As industries race towards deploying 5G networks in operational settings, there is a need to conduct a security analysis of the 5G infrastructure in diverse domain areas. Universities can play a key role in conducting security risk assessments with the potential to uncover exploitable vulnerabilities that could affect the resilience of the 5G infrastructure. Collaboration between research groups in North American and European universities can lead to an international research testbed on which to conduct empirical validation of innovative security technologies.

B. Cyber Threat Intelligence Sharing

5G security cannot be under the exclusive purview of technical teams. When a cyber threat emerges, it is generally detected first by private actors or by the public. Therefore, for organisations to be swift in responding to a cyber threat requires the fast sharing of relevant information by those actors. This can be accomplished through an Information Sharing and Analysis Centre (ISAC) (ENISA, 2018). The problem is thus to develop a cyber-threat information sharing capability allowing authorised participants to share real-time Cyber Threat Information (CTI) within an ISAC. That capability also has to ensure trust, anonymity and security to all users both inside and outside the ISAC. The significance of cyber security information sharing has led governments and regulators to mandate or encourage such sharing.

In the US, the Cybersecurity Information Sharing Act (US Congress, 2015) incentivises collaborative sharing among private- and public-sector organisations by providing liability protection to the sharing parties. The EU has also launched several cross- and intra-sector initiatives to enhance member states’ capability for preparedness, cooperation, information exchange, coordination and response to cyber threats. ITU-T recommendation X.1215 also discusses how structured threat information expression (STIX) language can be used to support CTI and information sharing, such as knowledge of threats, vulnerabilities, incidents, risks and mitigations and their associated remedies (ITU-T, 2019). To ensure a successful CTI capability, there is also a need for a large number of participants who actively share cyber incidents. Limited participation in this information sharing can significantly impair the ability to manage cyber risks. For example, the DHS has reported that the limited number of participants that ingest cyber threat information is the main barrier to improving the quality of indicators that can provide actionable information to remediate cyber threats (Office of the Inspector General of the Intelligence Community, 2019).

The fundamental concerns of low participation in CTI sharing include lack of trustworthiness from the participating organisations, uncertain authenticity of the exchanged information, improper anonymity, the existence of free-riders, malicious insiders and the possibility of information tampering. Blockchain technology should be investigated for its potential for transparent and trusted information exchange that would give provenance for vendors’ and suppliers’ actions. An example of blockchain’s use for information sharing has been demonstrated by IBM’s Mission Partner Environment (MPE) (IBM, 2018). The MPE is empowered by blockchain private channels that allow the exchange of unclassified information between unclassified and classified networks. The MPE facilitates multinational information sharing and ensures the number and size of each shared MPE are essentially reduced to ledger. The shared private channel ledger capability lowers implementation costs through the reuse of existing MPE resources, increases sharing by enabling countries to use their indigenous technologies and provides accountability via immutable ledger and fine-grained lifecycle security control.

C. Expansion of Standardisation to the 5G Ecosystem

There will be a need for several standardisation efforts focused on secure 5G infrastructure and secure 5G-enabled use cases. Although 3GPP provides 5G infrastructure security specifications, there is a need for additional standard bodies at the intersection of 5G and technologies such as blockchain, IoT and autonomy. Public-private partnerships can be leveraged to develop de facto standards and promote best practices for 5G security implementation and 5G secure supply chains that other countries may come to adopt.

These efforts will benefit from government funding focused on realising: (i) standards-compliant network stacks for 5G and beyond that are opensource and secure by design to encourage the decoupling of the software and hardware ecosystems of 5G; these, in turn, will mitigate the threat posed by supply-chain attacks and promote 5G vendor diversification and market competition; (ii) innovation support for start-up companies; (iii) international collaboration and partnerships that create joint academic and research programmes centred on 5G; (iv) participation in standards bodies responsible for 5G and related technologies; and (v) exchange programs among leading research universities in NATO nations and its strategic partners such as South-Korea, Japan and Australia.

6. CONCLUSION

There is widespread awareness by governments and industry of the great potential for economic development that comes with 5G and of the new security vulnerabilities that come with it. More than in previous generations of mobile systems, there is also open discussion of the geopolitical factors in play. Specific concerns about security and privacy in the context of major Chinese 5G vendors have led to widely publicised discussions between US national security officials and their counterparts in allied nations.

The defence and national security apparatuses in many countries are grappling with how they can adopt 5G as part of their own critical communications infrastructure. In doing that, they face questions including military and civilian spectrum-sharing, adoption of open source implementation and securing the supply chain. It is appropriate, therefore, that NATO plays a role in 5G innovation and security by design, in sharing of 5G threat intelligence and in the certification of 5G security solutions.

We argue that increased cooperation among NATO nations and its strategic partners is vital to effectively face the new challenges brought by 5G. A role for NATO in serving as a forum for collaboration in 5G security across the Atlantic and expanding that collaboration through its diplomatic dialogues has also been recently advocated by others (Chivot and Jorge-Ricart, 2020). The development of a common 5G security strategy across the Atlantic would be the critical first step towards implementing the recommendations in this chapter. A common strategy, with buy-in from key stakeholders in government and industry, could lead to the creation of joint research programmes, harmonised spectrum allocation, a united front on the development of standards and incentives to accelerate intellectual property and innovation. 6G is already starting to be discussed: to regain the leadership in 5G and its successors, NATO nations will need to incentivise close collaboration between academic researchers, relevant NATO Centres of Excellence, NATO entities, private industry and regulators in NATO nations working together towards a common goal. Modest funding by the European Commission exists for international research collaboration in 5G, but this would need to be increased significantly with coordinated participation from funding agencies across the Atlantic to achieve the level of effect that we advocate in this article.

Such a joint strategy could also lead to more effective and coordinated participation by NATO nations and non-NATO EU member states in the standardisation of 5G and subsequent generations. It could also affect the adoption and success of new technologies, like open source initiatives for the 5G radio access network being championed by the O-RAN Alliance (2020) that can have a profound impact on the supply chain of these future networks.

#### Alliance-wide NATO standardization develops common guidelines and security standards for 5G networks and applications.

Oeselg ’22 [Veeli; June 2022; Partner at CIVITTA, M.Sc. in Business Administration from the University of Tartu; et al.; "Military Movement: Risks from 5G Networks," https://ccdcoe.org/uploads/2022/06/Report\_Military-Movement-Risks-from-5G-Networks.pdf]

6. Recommendations

It is essential in cybersecurity management that security comes first in relation to people, processes, and technologies. This requires specific operational technology, cybersecurity practices, and adapted design characteristic of the solutions. By 2030, it is expected that 5G roll-out will be widespread and many new use cases will have emerged. Even if many industries see no potential in 5G applications, 5G networks will revolutionise our society, including the way we move military assets. Even though military movement will likely maintain a low level of adoption of direct use of 5G technology – automation and seamless data integration will still increase the speed, efficiency, and observability aspects of asset movements, and decrease maintenance costs and environmental impact. But if NATO member country militaries rely on civil third-party contractors for the movement of assets, the change towards 5G based solutions will happen one way or the other because civilian use cases will surpass the military with their level of 5G technology adoption. With these developments, major cybersecurity challenges will arise, and the value chain needs to take that into account.

6.1 Policies and Standards

Military and policymakers need to be knowledgeable about the possibilities of technology, including what 5G provides for military movement in the pursuit of closer cooperation on policies and standards. NATO will need to address the potential vulnerabilities of the new generation networks with a specific goal to assure that next generation networks will be secure. To ensure the interoperability and cyber safety of military-related use cases, NATO and EU member states should adopt policies and standards that are harmonised between countries related to approval and auditing of available hardware and software solutions used in private 5G networks. However, as NATO has no direct power over creating regulations and standards, certain favourable guidelines should be created directed towards member countries to implement within the jurisdiction of the National Regulative Authorities. As the created 5G network should be end-to-end secure by design, following internationally set standards, it is advisable that NATO jointly with EU authorities evaluate the feasibility of creation/use of trusted (virtual) mobile network operators for military transportation operations. As the big MNOs that are responsible for public 5G networks have considerable power over respective agencies and institutions responsible for creating the standards, NATO should be in close cooperation with different authorities and MNOs. It is feasible to develop European scale technical and legal solutions together with MNOs for on-demand deactivating of certain vulnerable ITS services during military movements. The specific vulnerabilities and risk levels must be identified through specific analysis and studies, possibly within EU research and development projects. All risks related to the implementation need to be considered from the start of the use case development phase. Even though the military is more conservative regarding changes to culture and operational practice compared to the commercial sector, technological developments will inevitably reach the operational phase.

6.2 System Security

To mitigate risks related to 5G system security, the interested parties, most notably NATO and EU member states, must be proactive in planning, be engaged in commercial development, as well as be stringent in monitoring and enforcement. These aims can be achieved through the following three recommendations:

DEVELOP A COMPREHENSIVE 5G CYBERSECURITY STRATEGY | As the military will interact with the rapidly developing 5G ecosystem, NATO will have to develop a comprehensive cybersecurity strategy by mapping out the various forms of interactions, corresponding risks, and adequate responses. In the strategy, all military movement needs must be identified, infrastructure enabling the movement must be mapped and its technological composition evaluated. Based on that mapping, all the opportunities and risks related to the intersection of future military movement and 5G development should be highlighted with recommendations developed by military and technological experts. The strategy would facilitate making Alliance-wide strategic decisions regarding 5G-use, including recommendations to private 5G network owners and intelligent transportation system providers. Given that security management will become essential in handling ongoing threats and risks, a proactive plan for the security management cannot be developed before a comprehensive cybersecurity strategy is in place.

ENGAGE IN BUILDING SECURE SYSTEMS AND 5G NETWORKS FROM THE BEGINNING | The commercial 5G systems that the military will interact with in the future are being built now. It is imperative that these systems and 5G networks are being built in a secure manner from the start. NATO, in close cooperation with the EU member countries and their regulative authorities, should take a proactive stance in the development process and strongly recommend certain guidelines to its commercial partners regarding the military-related security needs both for vendors and MNOs. Shaping the development process to security priorities as it happens is more convenient and cheaper than coming up with risk management measures retrospectively in a reactive manner. For this, it would be advisable to create a list of security approved 5G RAN devices or vendors at a national or EU level as it is possible industrial enterprises or even MNOs might not be aware of possible security issues for specific hardware components.

ADOPT STRINGENT MONITORING AND SECURITY ENFORCEMENT PROCESSES | When fully operational, all relevant parties need to run frequent and structured risk analysis to assess the security of the systems and to avoid any potential risks or threats that might arise. Upon the installation or design of the system, the underlying report can be used for auditing purposes if all the necessary steps have been followed (see Chapter 5.3). As NATO will be relying mostly on the private sector, companies as logistical partners are strongly advised to follow policy recommendations as collectively agreed in NATO and in cooperation with the EU. For that, the NATO Standardization Office could be responsible developing such requirements. The first step of which would be to consider how the current 3GPP standards address the security requirements of the military. NATO Allies should cooperate in assessing and certifying hardware and software products, processes, and services associated with 5G technology according to jointly agreed criteria, consider the existing certification schemes, and assess their value and sufficiency. Upon the completion of the requirements, companies should be encouraged to meet a set of standards in order to provide any services to NATO related military movement. This also means that NATO should provide the guidelines to and lobby national governments who will need to be active in communicating and monitoring the fulfilment of these requirements.

6.3 Recommendations Related to Use Cases

Based on the case studies of smart seaports and road transportation presented, the 5G-enabled use cases carry both increased opportunities as well as risks. Therefore, for each use case, the military must (in the previously suggested cybersecurity strategy) conduct a systematic and professional risk analysis weighing the potential advantages of technology adoption against the disadvantages of increased risk. The risk analysis must conclude where the advantages outweigh the disadvantages, or the upside is high enough to take on the downside risk. It is not predicted that dedicated military vehicles will extensively interact over 5G networks in given timeframe up until 2030. The risks are related to services provided by civil infrastructure – both at ports and on roads – and contracted vehicles. Having said that, the current analysis concludes with the following recommendations for supply chain security of the two case studies.

#### NATO standards maximize upsides of commercial and military 5G applications while minimizing risk.

Kertysova ’21 [Katarina; February 2021; Policy Fellow at the European Leadership Network, Wilson Center Global Fellow, M.A. in French and International Relations from the University of St. Andrews, M.A. in International Security from Sciences Po Paris; et al.; "When 5G Meets AI: Next Generation of Communication and Information Sharing," https://stratcomcoe.org/publications/when-5g-meets-ai-next-generation-of-communication-and-information-sharing/237]

As this paper demonstrates, the development of 5G is a double-edged sword for democratic societies. On the one hand, 5G will enable greater connectivity and access to information, which promises to improve democratic participation, activism, and citizen mobilization. On the other hand, it can be used by governments to tighten information control, repress political opponents, and manipulate public opinion. The technology itself is inherently neutral; it is only what we, users, do with it that determines its impact.

Though widespread adoption will not be realized for a few years, once fully adopted, 5G will allow us to communicate ideas instantly, redefine audience engagement, and deliver unprecedented targeting capabilities. It will also change the way we interact with (political) advertising. 5G will bring to life new applications and usages: moving communication from a 2D to a 3D holographic format, enhancing video and voice calls, AR and VR, and providing richer and more interactive experiences. High-resolution audio and visual material will enable users to interact in ways that 4G does not come close to.67

5G has the potential to fill the gaps left unaddressed by previous technological revolutions. The changes that come with the implementation of 5G technology have the potential to considerably accelerate machine-tomachine interaction, but it remains to be seen how exactly it will impact human-to-human communication. While 5G is unlikely to usher in another major communications revolution, it would be naive to assume that nothing will change.68

Especially regarding disinformation campaigns, 5G will not only introduce new risks but also aggravate existing ones. First, a feature unique to 5G is its ability to collect new kinds of user data (such as more precise localization, biometric, and sensorial data), which can be used for more effective user profiling and (psychometric) targeting of those who are most vulnerable to influence. Second, 5G-backed AI capabilities will make it possible to manipulate audio-visual content in real time, making deepfakes more convincing. At the same time, because of its speed and connectivity, 5G will enhance all the problems we have been grappling with for the past decade. Not just the news, but also disinformation that journalists must sift through will travel faster and spread more widely in the era of 5G. As put by the Belfer Center for Science and International Affairs at Harvard: ‘the weaponization of information through speedier channels could pose a threat to knowledge and information integrity’.69 If even more information about a person’s environment becomes accessible, the potential for misuse expands too. Problems caused by previous technological breakthroughs plaguing social media today have not been solved. 5G and AI are evolving at such a quick pace that existing problems are likely to permeate, and intensify, in the 5G era.

Recommendations

1. Address the potential for data misuse. The first challenge lies in ensuring that personal data is secure – a challenge that is not unique to 5G networks. This necessitates both technological and regulatory solutions. On the technological side, privacy by design solutions and disclosure measures, i.e. getting companies to disclose how personal data is collected and what it is being used for, could minimize the risk of data misuse. On the regulatory side, improved law enforcement in 5G networks and adequate state policies that set out requirements for privacy regulations are needed. Such national strategies and policies should be harmonized across the Alliance. As tech companies such as Meta (previously Facebook), which have come under intense scrutiny for the mishandling of user data, turn to 5G to roll out new applications, it is crucial to promote greater accountability and address existing issues surrounding algorithmic transparency. In addressing these challenges, governments should ensure that regulation does not inhibit innovation and that democratic societies are not outpaced by their adversaries when it comes to technological advancement.

2. Address supply chain and network security issues. Modern militaries are going to become increasingly reliant on 5G for a wide variety of capabilities, from situational awareness, through military command and control (C2) and communications, to logistics. As connected devices proliferate, cybersecurity and resilience of 5G networks are crucial. Software supply chain efforts can address open-source vulnerabilities. To ensure the integrity of supply chains, technology vendors are increasingly adopting a zero trust network design. In May 2021, the Biden administration issued an executive order on zero trust architecture.70 While disruptive for companies, this authentication system makes cyberattacks much less effective. Another important step in this regard was the adoption of the EU Toolbox for 5G Security in January 2020, which allows only ‘trusted suppliers’ into EU member states’ networks. On the procurement side, it would be prudent for NATO to investigate the technologies that are being used in its systems and the civilian infrastructure that the military relies on, as well as their origins. To that end, NATO should develop common criteria to evaluate the trustworthiness of 5G vendors, technology, and infrastructure.

3. Adopt cyber and technology standards. With a long and successful track record as a standard-setter, NATO should be at the forefront of developing an ethical framework to drive the development and implementation of emerging and disruptive technologies, including 5G and AI.71 This would help offset China taking the lead in global standard setting. NATO recently launched an AI strategy which will set ethical guidelines around how to govern AI systems, and it is also exploring the potential of 5G for military applications.72 NATO’s baseline requirements for resilience already cover telecommunications, but Alliance-wide military-grade criteria to secure public and private 5G networks are yet to be developed.73 To avoid duplication of effort, as a first step, NATO should take stock of what already exists and collaborate with Allied standard-setting bodies. Even with non-Chinese suppliers, the armed forces of NATO member states will largely rely on networks and equipment that are available commercially, which presents additional risks and vulnerabilities. Security requirements for military communications, such as the need to avoid being geo-localized and jammed by an adversary, exceed those offered by commercial 5G service providers, which have different security concerns and needs.74 In addition to setting standards and technical specifications, Allied militaries should strive to secure high quality support and engineering, and closely cooperate with the industry to ensure that military-specific requirements are taken into consideration.

# Case---Solvency

## Mechanics

### Solvency---2AC

#### Cooperation among NATO solves hard and software 5G risks.

DaSilva ’20 [Luiz; December 2020; Bradley Professor of Cybersecurity and Executive Director Commonwealth Cyber Initiative at Virginia Technology, Ph.D. in Electrical Engineering from the University of Kansas; et al.; "Securing 5G: NATO’s Role in Collaborative Risk Assessment and Mitigation," <https://ccdcoe.org/uploads/2020/12/4-Securing-5G_ebook.pdf>]

1. INTRODUCTION

If any doubt remained about communication networks making up a key component of our critical infrastructure, the COVID-19 crisis has put it to rest. With the increased role that these networks play in keeping the economy going, new threats have emerged and existing ones intensified. For example, the healthcare industry has been experiencing a surge in ransomware attacks, with an increase of 350 per cent reported for the last quarter of 2019, a trend that has only worsened in 2020 (Corvus Insurance, 2020). With 5G networks starting to be deployed worldwide, there is justified concern about new cyber threats associated with this technology.

The introduction of any network technology creates the potential for new security attacks, but in some respects 5G is different. It builds on previous generations of cellular technology by improving the bandwidth, capacity, latency and reliability of mobile broadband services. With its promise to enable a new generation of services through ultra-reliable low-latency communications, 5G can also significantly expand the attack surface of the network (Frost and Sullivan, 2020). If applications such as smart homes and blended autonomous vehicles depend on 5G, an attack on the network can have safety-of-life consequences. The apparent dominance of Chinese vendors in the 5G space has also raised questions in the US and elsewhere about the level of independence of vendors from national governments (Iplytics, 2019).

Addressing both technical and geopolitical challenges in 5G security will require strong international cooperation that goes beyond the standardisation process that already takes place in the 3rd Generation Partnership Project (3GPP) and other standards bodies. We believe that this must include the development of international benchmarks for 5G security and a certification process for hardware and software to pass stringent security tests. Recent strides in artificial intelligence can be leveraged for the creation of automated tools to check for security vulnerabilities.

The core principles for 5G security can benefit strongly from international consensus and NATO member states can have a role in establishing the mechanisms for this consensus to emerge. Relevant metrics should be identified and tracked through an international 5G cyber security-focused Information Sharing and Analysis Centre (ISAC). An open vulnerabilities database should be created, thereby increasing transparency and affording industry, government and academic stakeholders access to shared information on those security threats plaguing the 5G infrastructure.

The geopolitical issues in the supply chain for 5G networks also require a coordinated approach. The open radio access network concept and, more broadly, the reliance upon 5G systems that are open by design, will encourage the disaggregation of those software and hardware ecosystems associated with 5G. This process has the potential to mitigate the threat posed by supply chain attacks and promote a diversification of 5G vendors.

The broad problem of cyber security in 5G can only be handled adequately through coordination between researchers, industry and policymakers from across the globe. With the strategic role that 5G is starting to play in national security and military organisations, NATO is well placed to facilitate this coordination. This article summarises unique security aspects brought about by the advent of 5G and presents recommendations for how the international community and NATO, in particular, can respond to these challenges.

2. 5G SECURITY: WHAT’S NEW?

The vision for 5G security includes security by design, flexibility to respond to new threats, and automated security systems leveraging artificial intelligence (Ahmad et al., 2019). The International Telecommunication Unit Telecommunication Standardisation Sector (ITU-T) has a number of study groups involved in drafting security standards and recommendations. These efforts are complemented by those of other international standardisation bodies such as the 3GPP, the European Telecommunications Standards Institute (ETSI) and the Internet Engineering Task Force (IETF).

Nevertheless, some unique concerns attach to the issue of security in 5G systems: a) the virtualisation of network functions and resources; b) the 5G pillars of massive machine-type and ultra-reliable, low-latency communications (Sexton et al., 2017); and c) concerns about the international supply chain for 5G equipment. These are summarised in Figure I.

First, softwarisation—that is, moving functionality that was traditionally provided in hardware to software—is a major trend in networks with the advent of Software Defined Network (SDN) and Software Defined Radio (SDR) and the replacement of network-specific hardware with white boxes. In 5G, this trend gains additional steam through a concept called slicing. Network virtualisation and slicing techniques enable the running of multiple logical networks as independent business operations on a common physical infrastructure (Afolabi et al., 2018). In essence, each network slice represents an independent virtualised end-to-end network and allows operators to deploy multiple services with distinct architectures in parallel over the same physical network. While virtualisation and slicing play a critical role in 5G systems, they also introduce potential security vulnerabilities due to the challenge of simultaneously providing strong resource isolation and efficient resource use in a virtualised environment. Exploiting the shared physical platforms in 5G infrastructure, adversaries could construct side channels or covert channels to impose serious security threats on 5G communications. Thus, it is essential to protect the slice-provisioning process in 5G infrastructures against malicious attacks and to ensure strong slice isolation.

Second, the specifications for 5G are built on three pillars: enhanced mobile broadband; Massive Machine Type Communications (MMTC); and Ultra-Reliable Low Latency (URLL) communications. The last two present a paradigm shift for wireless networks in terms of the need to scale massively (in the case of MMTC) and in the support of stringent reliability requirements (for URLL). They also expand the attack surface of the network to a new class of devices—sensors and Cyber Physical Systems (CPSs)—and services from autonomous transportation to Augmented and Virtual Reality (AR/VR). Attacks on those services can present safety-of-life risks: imagine, for example, a hacker taking control of an autonomous vehicle.

The third area of specific concern in 5G relates to the reliability and trustworthiness of the supply chain for those networks. Huawei Technologies currently leads in the number of declared 5G patent families (Iplytics, 2019), followed by Samsung and LG Electronics. Among the top ten companies in this category, only two are based in Europe (Nokia and Ericsson, in fourth and sixth positions, respectively) and two in the US (Qualcomm and Intel, in seventh and eighth, respectively). The geopolitics of 5G have dominated the news of late, with the US exerting pressure on its allies to not deploy 5G testbeds based on Huawei equipment. Concerns are around a close relationship between the vendor and the Chinese government, with the potential for privacy and security violations (Kaska et al., 2019).

The softwarisation and virtualisation of 5G, including the introduction of service orientation in the 5G ecosystem, bring advantages and disadvantages. The 5G architecture introduces mobile edge computing (Liu et al., 2018; Mao et al., 2017) as a key component of its architecture that will enable faster and diverse services for new use-cases such as e-health or connected autonomous vehicles. However, virtualised service-oriented architectures have a long history of vulnerabilities (Riaz & Tahir, 2018; Tank et al., 2019), kill chains (Kim et al., 2019; MITRE, 2020) and post-attack forensics (Sharevski, 2018). In addition, the newer application domains may connect their specialised equipment and controllers to 5G base stations. This makes vulnerability tracking and associated risk evaluation and post-attack forensic examinations more complex and issues such as supply chain security and attack attribution more challenging.

The deployment of 5G services will involve re-architecting the wireless cellular network with new capabilities such as software-defined networking, network function virtualisation and a cloud-native architecture. These enhancements bring the need for cyber defence in the edge, secure network slicing, secure multi-access edge computing and access control policies for a disaggregated radio access network.

In the next two sections, we propose a number of actions that can be taken to address these challenges and how NATO, together with the broader international community, can establish tighter collaboration in identifying and overcoming the security threats that may arise with this new technology.

### Solvency---AT: Spectrum Sharing---2AC

#### Spectrum is being harmonized now – coordination is possible

Norin et al ’22 [Mats, Norin holds an M.Sc in Mechanical Engineering from the Royal Institute of Technology, Stockholm, April 2022, "Whitepaper on 5G spectrum for industrial networks," Ericsson, <https://www.ericsson.com/en/reports-and-papers/white-papers/5g-spectrum-for-local-industrial-networks>, St. Mark’s, AM]

The European Commission (EC) has identified the demand for mid-band licensed spectrum for vertical users and other terrestrial wireless local area use cases. It has issued a Mandate to CEPT to investigate the shared use and harmonized frequency arrangement of the 3.8-4.2 GHz frequency band for local area connectivity [11]. The work is tasked to finish by March 2024, with reports delivered November 2022 and July 2023.

## Say No

### Solvency---AT: Say No---2AC

#### Consensus possible and necessary for NATO operations.

Gorman ’19 [Lindsay; 12/3/19; Fellow for Emerging Technologies at the Alliance for Securing Democracy, M.S. in Applied Physics from Stanford University; "NATO Should Count Spending on Secure 5G Towards Its 2% Goals," https://www.defenseone.com/ideas/2019/12/nato-should-count-secure-5g-spending-towards-its-2-goals/161648/]

The agenda at NATO’s London summit reportedly includes talk about the future of internet security — that is, establishing rules and roles for next-generation 5G gear. This is both a vital issue and a bellwether. If done right, moving to secure 5G systems can rejuvenate the alliance around its central mission: protecting democratic states from authoritarian incursion. Botch it, and the rift will only increase.

Whether NATO comes together or falls apart over 5G presents an initial test of how it will handle China’s rise. For Beijing, leapfrogging Western telecommunications firms is part and parcel of a vision to spread norms of authoritarian internet governance, promote surveillance technologies, build global dependencies, and undermine the liberal democratic order NATO anchors. U.S. officials can take several steps to help move the debate from admonition to action.

First, NATO should allow members to count a portion of outlays on secure 5G systems towards national 2-percent defense spending goals. There are a number of ways 5G-inclusive targets could be defined, including one-time commitments or line-item funds, but if investing in technology built by trustworthy vendors is a priority for the United States—and it should be—the alliance’s cost-sharing structure should reflect it.

Second, NATO should conduct thorough technical and political risk assessments on 5G networks and build shared cybersecurity standards. Last month, NATO announced plans to update rules for civilian 5G. The United States should use this process to push for transparency requirements on the companies that build 5G networks, including disclosures on corporate ownership structures, direct government funding, and state influence and control. Whether an authoritarian government subsidizes telecommunications equipment to undercut local competitors—or controls a company to steal military, commercial, or personal data—is relevant when considering allowing it to build the foundations of economic opportunity for NATO member states.

Put simply, NATO should require participating suppliers to show credible independence from foreign governments. In addition to helping secure networks, such a requirement fosters internet governance that resists authoritarian surveillance and erects barriers to the unfettered access of private citizen data.

Third, the United States should urge its allies to consider cooperative business models and infrastructure sharing arrangements that would help member countries choose trusted-yet-costlier systems over cheaper alternatives. Some creativity may be in order here, but NATO partnerships with the EU, Finland, and Sweden could build joint funding and research models for secure 5G and even 6G systems.

Proposing these initiatives would add constructive action to the U.S. government’s steady drumbeat against Huawei. Concerns over Chinese-made 5G have centered on espionage, but extend to amassing sensitive personal and corporate information and leveraging internet dependence for geopolitical control. In capital after capital, U.S. diplomats have warned allies and called for outright bans.

For the rest of NATO, these concrete steps are also more politically viable. Amid divisions within allied nations over 5G and ample pressure from China, a tenuous “plausible deniability” consensus may emerge: to ratchet up requirements without singling out one country or company. A recent European Union risk assessment on 5G, for example, notably cautioned against threats from state actors, but stopped short of naming China explicitly.

Disunity here has real consequences. A split over cybersecurity and the varying presence of “untrusted” suppliers from China in member countries’ 5G networks threatens vital NATO military and intelligence cooperation. The United States has already warned that it will limit intelligence sharing if allies build 5G networks with Chinese equipment. In the words of one official, “the Americans will assume that everything we share with Germany will end up with the Chinese.”

Such an outcome would be disastrous for the alliance. A NATO intelligence-sharing rift would open the door to greater authoritarian interference in Western democracies, and not just from China. NATO’s intelligence sharing and threat analysis cell is a central tenet of its plan to combat hybrid threats from Russia and others: disinformation campaigns, malign financial flows, the annexation of Crimea, and more. Given Russia’s long-standing goal of fracturing NATO, it’s no coincidence that Russian state media champions Huawei.

### Solvency---AT: Say No---China---1AR

#### NATO says yes---fear of China unites them.

Meia Nouwens, 2022; Senior Fellow for Chinese Defence Policy and Military Modernization at the International Institute for Strategic Studies, with an expertise in China’s international relations, regional strategic affairs, and cross-service defence analysis. M.A. of International Relations and Diplomacy from Leiden University (conjunction with the Clingendael Institute) and an MPhil in Modern Chinese Studies from the University of Oxford and Peking University. “NATO and China: Addressing new challenges” CSDS Policy Brief, Brussels School of Governance Center for Security, Diplomacy, and Strategy, 04/2022, https://brussels-school.be/sites/default/files/CSDS%20Policy%20brief\_2204.pdf//ekc

The illegal Russian attack on the Ukraine moved NATO into the centre of public attention as the freedom and security of its members is at stake. China’s rise and its support for Russia, although not as straightforward as expected, presents the alliance with an additional new challenge. China seems to be no longer “out of area”. Furthermore, Chinese investment into NATO allies’ critical infrastructure, its growing global economic and political influence, the modernisation of its military, its cyberattacks and participation in disinformation campaigns paired with its ambition to build capabilities for global reach are all factors that force NATO to deal with China within the alliance, as well as in the Indo-Pacific. This policy brief posits that NATO’s priorities should be, first, to forge consensus on key matters such as investment screening and critical infrastructure resilience at home, and, second, to consider how it can play a role in the IndoPacific.

The challenges that China poses to NATO

At the Madrid Summit in 2022, the North Atlantic Treaty Organization will define its core tasks and priorities for the 21st century. While NATO is expected to increase its attention to the Pacific, the war in the Ukraine will have an impact. Nevertheless, there is a growing unease within the alliance about China’s rise, economically and politically, impacting on NATO and on its partner countries in the Indo Pacific region.

The greater focus on China in the Strategic Concept has been under discussion within NATO and with allies since the mid 2000s. Military-to-military cooperation with the People’s Liberation Army began in 2007. In 2011, then-secretary general Anders Fogh Rasmussen supported engagement with China: He saw China, as a permanent member of the UN Security Council, playing an increasingly important role on the global stage, also as a partner for the alliance to achieve peace and stability.

Ahead of the North Atlantic Council at the level of heads of state and/or government in 2019, NATO Secretary General Jens Stoltenberg had announced that the 2019 Summit Communique would mention China for the first time in an official document – the 1999 Strategic Concept had not mentioned China – The 2021 NATO Brussels Summit Communique, in which the Alliance adopted its 2030 Agenda. Countering China’s various challenges to the alliance were the focus of the document as NATO seeks to address “China […] coming closer to [the alliance]”.

In the non-binding 2030 Reflection Report, and in NATO’s 2030 Agenda adopted in 2021, NATO officially stated its intention to work more alongside partners in the Indo-Pacific and tackle the political, economic, and military challenges China poses. However, the vast majority of these challenges fall within areas that are not traditionally NATO’s responsibility.

The 2030 Agenda highlights China’s military modernisation and to the creation of new capabilities in the cyber, space, maritime, and air domains. NATO voiced particular apprehension about China’s development of nuclear-capable systems, which are able to reach NATO countries, and about Xi Jinping’s government expanding its arsenal with “more warheads and a more sophisticated delivery system in an unrestricted manner”. This adds another nuclear threat to NATO beyond the traditional threat posed by Russia, which President Putin has recently raised when attacking Ukraine.

Though China has not used force against NATO, it “has proven its willingness to use force against its neighbours”. Consequently, NATO has to factor in China’s development of longer-range, more advanced, and larger arsenals when planning its own nuclear deterrence. The military cooperation between Russia and China poses additional concerns, as evidenced in the Ukraine War as well as by earlier joint-military drills in Russia and in the Euro-Atlantic region.

The 2030 Agenda is not limited to military considerations but identifies a broad range of challenges that China poses to the rules-based international order through its approach to human rights and international law. It identifies China’s use of economic coercion and intimidatory diplomacy, as well as disinformation efforts, as challenges to NATO’s unity, its collective resilience, the security of critical infrastructure (such as 5G), supply chains, and its ability to maintain an innovative edge in new technologies.

NATO places increasing importance on the development and adoption of technologies such as artificial intelligence (AI), autonomous weapons systems, biotechnology, quantum computing. Therefore, the protection of intellectual property rights and innovation in the academic and private sector have gained importance.

5G, where China made important inroads in the European critical infrastructure and digital ecosystems, is a particularly grave concern for NATO. The United States, supported by some allies, regards the integration of Chinese-built 5G networks across the alliance as a significant intelligence and operational risk. This could also endanger European innovation in strategic industries. Companies like Huawei have close links with the Chinese Communist Party and according to Chinese laws could be pressured to reveal information about their overseas engagements. US officials contend that any information flowing through Chinese 5G networks could be compromised through Beijing’s use of backdoors built into the code of the technology.

In the economic sphere, the Reflection Report contends, NATO Allies will continue to diverge as governments attempt to strike a balance between the need for security and the desire for economic benefits through access to the Chinese market. While the 2030 Agenda underscores the need for unity within the alliance, the Reflection Report highlighted that political unity across the alliance is at present still a ‘work in progress’ on how to address future challenges, including national economic interests. As the report warns, China will continue to exploit this division among allies in its own interests.

### Solvency---AT: Say No---Albania

#### Albania says yes.

Dave Nyczepir 21, technology reporter for FedScoop, 6/13/2021, "US, Albania agree to develop secure 5G networks abroad," FedScoop, <https://www.fedscoop.com/us-albania-5g-network-agreement/>, RMax

The U.S. and Albania agreed Sunday to coordinate development of secure 4G and 5G networks abroad, as the former tries to stop Western Balkans countries from buying potentially compromised Chinese infrastructure.

Without mentioning China by name, both parties acknowledged the threat foreign adversaries pose to the telecommunications supply chain.

In recent years the U.S. has struck similar agreements with the Western Balkans countries of Serbia, Kosovo and North Macedonia to assess the risk of 5G equipment supplied by vendors with connections to foreign adversaries, namely Huawei and ZTE, before buying.

“I think we’re setting a very strong example together here today, particularly on the need to make sure that when it comes to our most sensitive technology and networks, we’re working with trusted vendors,” said Secretary of State Antony Blinken.

Blinken signed the memorandum of understanding with Albanian Prime Minister Edi Rama, noting the partnership between the two countries was “growing stronger, growing deeper.”

### Solvency---AT: Say No---Belgium

#### Belgium says yes.

Supantha Mukherjee 20, and Mathieu Rosemain, journalists for Reuters, 10/9/2020, "Huawei ousted from heart of EU as Nokia wins Belgian 5G contracts," U.S., <https://www.reuters.com/article/us-orange-nokia-security-5g-idINKBN26U0YY>, RMax

STOCKHOLM/PARIS (Reuters) - Orange and Proximus have picked Nokia to help build 5G networks in Belgium as they drop Huawei amid U.S. pressure to exclude the Chinese firm from supplying key telecoms equipment.

The moves are among the first by commercial operators in Europe to drop Huawei from next-generation networks and come after months of diplomatic pressure from Washington, which alleges Huawei equipment could be used by Beijing for spying.

The Belgian capital Brussels is home to the NATO alliance and the European Union’s executive and parliament, making it a matter of particular concern for U.S. intelligence agencies.

“Belgium has been 100% reliant on Chinese vendors for its radio networks - and people working at NATO and the EU were making mobile phone calls on these networks,” said John Strand, an independent Danish telecoms consultant.

“The operators are sending a signal that it’s important to have access to safe networks.”

The United States welcomed the decisions by Orange Belgium and Proximus, which have a network sharing agreement.

### Solvency---AT: Say No---Bulgaria

#### Bulgaria says yes.

Reuters 20 – Reuters Staff, 10/23/2020, "Bulgaria signs 5G security declaration with U.S.," U.S., <https://www.reuters.com/article/us-bulgaria-usa-5g/bulgaria-signs-5g-security-declaration-with-u-s-idUSKBN2782X9>, RMax

SOFIA (Reuters) - Bulgaria and the United States signed on Friday a declaration on security of next generation 5G mobile telecoms networks, which should ensure protected and clean communications, officials said on Friday.

Bulgaria has joined the U.S. State Department’s Clean Network initiative, which says it seeks to eliminate “long-term threats to data privacy, security, and human rights posed to the free world from authoritarian malign actors, such as the Chinese Communist Party”.

“Bulgaria is in a good company. As a member of the NATO Alliance it now joins 27 of the 30 NATO member states as a member of the Clean Network”, said Keith Krach, U.S. undersecretary for economic affairs in a video released by the Bulgarian government from the signing.

The U.S. embassy in Sofia called the signing “historic” and said Bulgaria was joining a “growing coalition of countries and companies committed to protecting their 5G networks from untrusted vendors”.

Washington has been alarmed by Beijing’s dominance in the 5G infrastructure market and has pressed its allies to exclude China’s Huawei Technologies.

Bulgarian Prime Minister Boyko Borissov said the European Union has already provided guidelines on 5G network security and that they should be built on fair competition and transparency.

The government’s statement did not mention any specific vendors or what the document would mean for Bulgarian telecoms operators that will develop the 5G networks.

But Bulgarian business newspaper Kapital quoted Krach as saying the main idea of the initiative was to ensure the Bulgarian telecoms operators will use trusted vendors and would not choose Huawei and ZTE.

#### They welcomed Ericcson and Nokia.

Joe O’Halloran 21, reporter for Computer Weekly, 8/1/2021, "A1 selects Nokia, Ericsson tech for service roll-outs across middle Europe," <https://www.computerweekly.com/news/252505681/A1-selects-Nokia-Ericsson-tech-for-service-rollouts-across-middle-Europe>, RMax

A1 Telekom Austria Group has chosen Scandinavian network equipment suppliers Nokia and Ericsson as partners in the roll-out of 5G networks in the markets of Bulgaria, Croatia, Serbia and Slovenia.

A1 supplies digital services and communications systems in Central and Eastern Europe with about 25 million customers, currently operating in seven countries – Austria, Bulgaria, Croatia, Belarus, Slovenia, North Macedonia and Serbia.

Nokia and Ericsson are already longstanding strategic partners for the operator. By selecting them, A1 Telekom Austria Group took a decision to evolve its networks and services, said Alexander Kuchar, director group technology and future services. “We are demonstrating a strong commitment to providing the best user experience in terms of communications and entertainment services on a high-class and secure infrastructure to our B2C and B2B customers,” he said. “At the same time, we are taking a strong stand on virtualisation, automation and simplification of our network architecture.”

In Bulgaria, Nokia is building the radio network and Ericsson the core network; in Croatia, Ericsson is responsible for both radio and core network; in Serbia and Slovenia, Nokia is responsible for both radio and packet core network. In Austria, it was announced in spring 2019 that Nokia would be the chosen partner in the 5G roll-out of both radio and core network domains.

### Solvency---AT: Say No---Canada

#### Trudeau wants 5G cybersecurity---recent statements prove intent but don’t solve.

CP 22 – The Canadian Press, 5/23/2022, "Trudeau pledges more action on cybersecurity following decision to ban Huawei from 5G," constructconnect, <https://canada.constructconnect.com/dcn/news/government/2022/05/trudeau-pledges-more-action-on-cybersecurity-following-decision-to-ban-huawei-from-5g>, RMax

OTTAWA – A day after the federal Liberals banned Chinese firms Huawei Technologies and ZTE from helping build Canada’s 5G networks, Prime Minister Justin Trudeau says more must be done to secure critical systems against threats.

Trudeau says the government is working closely with big financial institutions as well as other companies across the country to protect vital networks from malicious attackers.

Speaking to reporters today, he says Canada will do more, whether through legislation, new spending or better and stronger partnerships.

Public Safety Minister Marco Mendicino said the government would table legislation to protect critical infrastructure in the finance, telecommunications, energy and transport sectors.

Fen Hampson, a professor of international affairs at Carleton University, says much of the “hidden wiring” of the Canadian economy lies in private hands, and securing it poses a huge challenge.

Hampson says the announcement on 5G does not resolve Canada’s security problems.

### Solvency---AT: Say No---Croatia

#### Croatia says yes.

Joe O’Halloran 21, reporter for Computer Weekly, 8/1/2021, "A1 selects Nokia, Ericsson tech for service roll-outs across middle Europe," <https://www.computerweekly.com/news/252505681/A1-selects-Nokia-Ericsson-tech-for-service-rollouts-across-middle-Europe>, RMax

A1 Telekom Austria Group has chosen Scandinavian network equipment suppliers Nokia and Ericsson as partners in the roll-out of 5G networks in the markets of Bulgaria, Croatia, Serbia and Slovenia.

A1 supplies digital services and communications systems in Central and Eastern Europe with about 25 million customers, currently operating in seven countries – Austria, Bulgaria, Croatia, Belarus, Slovenia, North Macedonia and Serbia.

Nokia and Ericsson are already longstanding strategic partners for the operator. By selecting them, A1 Telekom Austria Group took a decision to evolve its networks and services, said Alexander Kuchar, director group technology and future services. “We are demonstrating a strong commitment to providing the best user experience in terms of communications and entertainment services on a high-class and secure infrastructure to our B2C and B2B customers,” he said. “At the same time, we are taking a strong stand on virtualisation, automation and simplification of our network architecture.”

In Bulgaria, Nokia is building the radio network and Ericsson the core network; in Croatia, Ericsson is responsible for both radio and core network; in Serbia and Slovenia, Nokia is responsible for both radio and packet core network. In Austria, it was announced in spring 2019 that Nokia would be the chosen partner in the 5G roll-out of both radio and core network domains.

### Solvency---AT: Say No---Czechia

#### Czechia wants more 5G security cooperation in NATO.

NÚKIB 20 -- The National Cyber and Information Security Agency of the Czech Republic, 5/7/2020, "National Cyber and Information Security Agency," No Publication, <https://www.nukib.cz/en/infoservis-en/news/1660-czech-republic-us-want-to-cooperate-on-5g-network-security/>, RMax

On May 6, 2020, Czech Prime Minister Andrej Babiš and US Secretary of State Mike Pompeo signed the Mutual Declaration on 5G Network Security that included the goals of working together to increase the security of future fifth generation networks; creating mechanisms for finding reliable and trustworthy suppliers of software and hardware; protecting communication networks from possible violations and manipulation; and especially to provide citizens with protection of their privacy and individual rights.

As both leaders said, future 5G networks will allow for unprecedented development of new services and technologies, but they will also offer services necessary for the operation of states and often for the protection of the lives and health of inhabitants.

The goal of the declaration is to build 5G networks together so they are protected from unauthorized access and possible attack while also providing citizens with protection of their privacy and basic rights.

“5G networks are not just a huge opportunity to develop and modernize the economy and society, but also a series of security challenges. 5G networks will be a global phenomenon, which is why the state has to cooperate with partners within the EU, NATO, and other organizations in assuring security. The signature of the Czech-US declaration will greatly contribute to this goal just like last year’s announcement of the Prague Proposals or the European 5G Security Toolbox, which the Czech Republic played a pivotal role preparing. I’m proud that thanks to the NÚKIB’s contribution, the Czech Republic is seen abroad as a significant and respected partner in the area of cybersecurity,” NÚKIB Director Karel Řehka said.

The declaration is an extension of a number of documents that were adopted at the European Union level. These include the 5G Security Toolbox, which was adopted by the EU at the beginning of this year and which the Czech Republic significantly contributed to. Another document is the Prague Proposals announced at the Prague 5G Security Conference that took place on May 2-3, 2019, in Prague under the auspices of Czech Prime Minister Andrej Babiš. These documents, just like the newly-signed declaration, emphasize the need to build and implement 5G networks based on free and fair competition, transparency, and the rule of law.

According to the declaration, the following is especially important to evaluate:

    Whether the supplier is not under excessive foreign influence without the opportunity for independent legal review;

    Whether the supplier has a transparent ownership structure, traceable commercial relationships, and a standard management structure;

    Whether the supplier commits to regularly innovating its products and whether it respects intellectual property rights;

    Whether the hardware and software supplier acts in accordance with ethical standards for corporate behaviour and whether they are part of a legal environment that demands corporations behave transparently.

Representatives of both countries also declared the process of selecting trustworthy suppliers will not only contribute to increased national security, but it is also an opportunity for the further development and innovation in the private sector. Both countries also expressed support for further discussions about the security of 5G networks within NATO.

### Solvency---AT: Say No---Denmark

#### Denmark says yes.

Reuters 20 – Reuters Staff 6/8/2020, "Denmark wants 5G suppliers from closely allied countries, says defence minister," U.S., <https://www.reuters.com/article/us-telecoms-5g-denmark/denmark-wants-5g-suppliers-from-closely-allied-countries-says-defence-minister-idUSKBN23F1IT>, RMax

COPENHAGEN (Reuters) - Denmark wants to be able to exclude 5G technology suppliers from providing critical infrastructure in Denmark if they are not from countries considered security allies, online technology news outlet ITWatch reported on Monday.

“In order to protect Denmark and the Danes, we want to collaborate with someone with whom we already have alliances,” Minister of Defence Trine Bramsen told ITWatch.

### Solvency---AT: Say No---Estonia

#### Estonia says yes.

MFA 21 – Ministry of Foreign Affairs of Estonia, 1/15/2021, "Estonia and the United States funding effort on 5G military mobility," No Publication, <https://vm.ee/et/node/53899>, RMax

In late January, the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE) launches an initiative focused on the security of fifth generation (5G) telecommunications networks with the aim to analyse 5G security in the context of military mobility. The international team at the CCDCOE was awarded funding by both the US Department of Defence and the Ministry of Foreign Affairs of Estonia, and its first stage spans one year.

Foreign Minister Urmas Reinsalu said the security of communications networks is not only a technical matter, but also a strategic security issue. “The CCDCOE´s 5G project is the result of the work of Estonian diplomats and it gives an opportunity to develop NATO’s threat perception in the area of 5G security and an understanding how potential risks can be mitigated and prevented with technical standards for 5G and subsequent networks,” Reinsalu said. “We are still at the start of the project but there is potential for long-term cooperation between Estonia and the United States on such a critical issue of the future.”

Colonel Jaak Tarien, the Director of the CCDCOE, emphasised that in the immediate future, the collective defence capabilities of the Alliance would be increasingly reliant on commercial communications networks. “We do not want to be in a situation where the military or peacetime deployment of NATO forces is vulnerable due to insufficient security standards or malignant cyber activity,” Tarien added. “Thanks to our experience with engaging the private sector and our international team that includes most NATO member states as well as our partners from across the world, our centre is best placed to carry out this crucial research.”

One of the objectives of the project is to increase a common understanding among NATO Allies and partners that mitigating the security risks related to adopting 5G networks should be a part of strategic dialogue on all political levels.

5G security is an important area of bilateral cooperation between Estonia and the United States. In October 2019, US Vice President Mike Pence and Estonian Prime Minister Jüri Ratas signed a joint declaration on 5G security to highlight the risks related to 5G.

### Solvency---AT: Say No---Finland

#### Finland says yes.

Kati Pohjanpalo 20, Bureau Chief in Helsinki for Bloomberg News, 12/7/2020, "Home of Nokia Passes 5G Security Law Banning Suspect Gear," Bloomberg, <https://www.bloomberg.com/news/articles/2020-12-07/home-of-nokia-is-set-to-pass-5g-security-law-locking-out-vendors?srnd=technology-vp>, RMax

The home of 5G network-maker Nokia Oyj is introducing a telecommunications law which may be used to exclude China’s Huawei Technologies Co. and ZTE Corp. from its networks.

Finland’s parliament on Monday approved the bill designed to protect its networks against cyber threats and espionage. The legislation names no specific companies or countries, but bans equipment “within the network’s key assets if there are strong grounds to suspect the use of such equipment would endanger national security or defense.”

### Solvency---AT: Say No---France

#### France wants to keep Huawei out of critical networks.

Helene Fouquet 21, reporter for Bloomberg News based in Paris, 3/1/2021, "France’s Huawei Ban Begins to Kick In With Purge in Urban Areas," Bloomberg, <https://www.bloomberg.com/news/articles/2021-03-01/france-s-huawei-ban-begins-to-kick-in-with-purge-in-urban-areas?srnd=technology-vp>, RMax

Phone companies including Altice Europe NV’s SFR unit and Bouygues Telecom have begun removing Huawei Technologies Co.’s wireless equipment from large French cities after the government moved to purge the Chinese vendor from all but isolated parts of the country.

The work started at the beginning of 2021, when France’s Constitutional Council signed off on a ruling that forces carriers to rip out Huawei gear in densely populated areas where networks are being upgraded to fifth-generation wireless technology, according to people familiar with the situation.

Unlike countries such as the U.K., France is seeking to strike a middle ground that would allow Huawei to remain a supplier while keeping it out of the more integral parts of its wireless infrastructure. President Emmanuel Macron’s government has devised rules making it riskier for operators to use Huawei 5G kit.

Altice and Bouygues declined to comment. Huawei didn’t immediately return a call for comment.

In July, the head of the country’s cybersecurity agency said it will grant time-limited waivers on 5G for wireless operators that use Huawei products, a decision that will likely begin a “phasing out” of the company’s products. Macron has broadened those exclusions under pressure from the U.S., which sees Huawei as beholden to the Chinese Communist Party and a threat to national security.

To be able to deploy new mobile networks, Altice and Bouygues have now begun removing Huawei 4G equipment in a number of cities -- including Toulouse, Toulon, Rennes and Brest -- as it’s incompatible with the 5G kit they plan to install from other vendors, said the people, who asked not to be identified as the specific locations are not public.

#### They’re already phasing it out.

Mathieu Rosemain 20, reporter for Reuters, 7/22/2020, "Exclusive: French limits on Huawei 5G equipment amount to de facto ban by 2028," U.S., https://www.reuters.com/article/us-france-huawei-5g-security-exclusive/exclusive-french-limits-on-huawei-5g-equipment-amount-to-de-facto-ban-by-2028-idUSKCN24N26R, RMax

French authorities have told telecoms operators planning to buy Huawei 5G equipment that they won’t be able to renew licences for the gear once they expire, effectively phasing the Chinese firm out of mobile networks, three sources close to the matter said.

Like other countries in Europe, France is laying the ground for its next-generation 5G mobile market in the middle of a growing geopolitical storm between two global superpowers.

The United States say the company’s equipment could be used by the Chinese government for espionage - a charge denied by Huawei and Beijing - and has pressed its allies to ban it.

France’s cybersecurity agency ANSSI said this month it would allow operators to use equipment, including Huawei’s, under licences of three to eight years. But it added it was urging telcos not currently using the Chinese company’s gear to avoid switching to it.

### Solvency---AT: Say No---Greece

#### Greece says yes.

Erik Brattberg 21, director of the Europe Program and a fellow at the Carnegie Endowment for International Peace; et al., 10/13/2021, "China’s Influence in Southeastern, Central, and Eastern Europe: Vulnerabilities and Resilience in Four Countries," <https://carnegieendowment.org/2021/10/13/china-s-influence-in-southeastern-central-and-eastern-europe-vulnerabilities-and-resilience-in-four-countries-pub-85415>, RMax

Several Sino-Greek business deals have also been interrupted, if not outright canceled. In 2016, COSCO surprisingly stayed out of the race to privatize Greece’s railway operator TrainOSE, despite Premier Li Keqiang’s earlier interest. In 2018, the National Bank of Greece severed its negotiations with Gongbao for the sale of Ethniki Asfalistiki, the country’s largest insurance company.42 Five years after signing a $200 million investment agreement, real estate and financial group Fosun International withdrew in 2019 from a massive project to develop the former Hellenikon airport, apparently due to “years of delays caused by red tape and the country’s economic crisis.”43 Tellingly, the Chinese consortium was not entitled to bid for a gambling license that was eventually awarded to the U.S.-based Mohegan group and Greek construction company Gek Terna. More recently, in January 2021, the Greek government did not allow China’s State Grid (which already held a 24 percent stake in Greece’s high-voltage Independent Power Transmission Operator) to bid for a 49 percent stake in the country’s mid/low-voltage distribution network operator. Another Chinese state-owned enterprise, South Power Grid, was also disqualified. Lastly, the Greek government is leaning strongly toward non-Chinese suppliers for 5G technology. In March 2021, Cosmote, the largest Greek mobile service provider, selected Swedish telecommunications company Ericsson as its exclusive 5G equipment supplier. Greece also joined the U.S.-led Clean Network, an initiative on 5G launched by former president Donald Trump’s administration.44

### Solvency---AT: Say No---Hungary

#### Hungary is welcoming Ericcson.

Catherine Sbeglia Nin 20, managing editor for RCR Wireless News and Enterprise IoT Insights, 4/20/2020, "Ericsson and Magyar Telekom deliver 5G to Hungary," RCR Wireless News, <https://www.rcrwireless.com/20200420/business/ericsson-magyar-telekom-5g-hungary>, RMax

The new 5G network in Hungary uses the spectrum in the 3.6 GHz frequency range

Last week, Magyar Telekom and Ericsson officially brought 5G to Hungary, launching intial services in parts of Budapest, the town of Zalaegerszeg and Magyar Telekom’s headquarters in Könyves Kálmán körút. The collaboration is an extension of a longstanding partnership that already included the establishment of 2G, 3G and 4G networks.

The new 5G network uses the spectrum in the 3.6 GHz frequency range that Magyar Telekom’s recently acquired in the country’s [spectrum auction on March 26](https://www.mobileworldlive.com/featured-content/top-three/hungarian-operators-splurge-400m-on-5g/), which raised $400 million.

According to Tibor Rékasi, CEO, Magyar Telekom, the operator has been making 5G arrangements for a long time, including working with Ericsson on the operation of a six-month 5G test network.

#### Even if they’re hesitant, they’ll bend to US pressure.

Panyi Szabolcs 20, reporter for Direkt36, 7/3/2020, "Huawei is slowly pushed out from European 5G networks but the Orban government still supports them," Direkt36, <https://www.direkt36.hu/en/elkezdtek-kiszoritani-a-huaweit-europa-5g-halozataibol-de-az-orban-kormany-meg-kitart-a-kinai-ceg-mellett/>, RMax

Meanwhile, the deadline of 30 June has passed, which was when European Union member states should have announced individually the extent to which they would or would not limit the presence of so-called high-risk vendors in 5G networks. This also affects mobile operator’s vendor tenders. Although the Hungarian government has not previously raised any objections to the presence of Chinese telecommunications companies in Hungary, the parent companies of mobile operators typically decide for or against Huawei on the basis of global and regional, not just country-specific considerations. “Every country, especially the small ones, and every market player is waiting for what Germany will decide,” an official from a vendor company said. “Mobile operators will look at what decision each member state makes, but even if they allow Huawei to be present in that country, they will also look at how much political pressure the U.S. will put on them in other countries, especially in big markets. This means that things are not looking good for Huawei,” the source added. However, the German decision that everyone is waiting for has been postponed until at least September 2020.

### Solvency---AT: Say No---Iceland

#### Iceland says yes.

Ericcson 21, 5/3/2021, "Iceland's Síminn selects Ericsson 5G," <https://www.ericsson.com/en/news/3/2021/icelands-siminn-selects-ericsson-5g>, RMax

Building on Ericsson and Síminn’s long-term partnership, the new 5G deal will help to enable the next generation of innovation in Iceland. 5G RAN products and solutions from the Ericsson Radio System portfolio, including Ericsson Spectrum Sharing will be deployed.

The journey to 5G began when the companies conducted 5G trials as a part of a network modernization initiative.

Síminn will deploy 5G on 3.5-3.6GHz mid-band spectrum. The mid-band 5G deployment significantly enhances throughput to unlock the full potential of 5G. It can also be the key to unlocking a huge range of new opportunities in areas such as gaming, transport and manufacturing.

5G technology is designed to handle anticipated network capacity in the future - mobile data traffic in Europe alone is set to grow by more than 30 percent every year until 2025.

According to the latest Ericsson Mobility Report, 5G is expected to be the fastest deployed mobile communication technology in history and is forecast to cover about 60 percent of the world’s population in 2026.

Síminn aims to reach nationwide coverage by the end of 2022. Síminn 5G's deployment will begin by using of one of the legacy bands for low-band 5G, which enables wider coverage.

Erik Figueras Torras, CTO, Síminn, says: “Building on our good and long-standing partnership with Ericsson means that we’re able to foster innovation in new and exciting ways. With 5G we will be able to create new opportunities for Síminn, our customers, and the environment by adding even more value to our network infrastructure and services.“

He adds: “We can start looking even more at a digital future and capitalize on 5G-driven experiences from industry 4.0 opportunities to transforming how our customers and travelers to Iceland interact with Iceland’s cultural and natural offering.”

Jenny Lindqvist, Head of Ericssom Northern and Central Europe, says: “This deal confirms the promising development of 5G in Iceland. As tourism is the most significant industry in Iceland, 5G opens up a range of opportunities, particularly in the areas of audiovisual and augmented reality. We’ve already seen innovative benefits with immersive outdoor and digital experiences. It also positions Síminn as a reliable provider of 5G and gives their customers the confidence that they are getting best-in-class technology and service.”

### Solvency---AT: Say No---Italy

#### Recent actions prove.

Giuseppe Fonte 20, reporter for Reuters, 10/23/2020, "Italy vetoes 5G deal between Fastweb and China's Huawei: sources," U.S., <https://www.reuters.com/article/us-huawei-italy-5g/italy-vetoes-5g-deal-between-fastweb-and-chinas-huawei-sources-idUSKBN2782A5>, RMax

Italy has prevented telecoms group Fastweb from signing a deal for Huawei [HWT.UL] to supply equipment for its 5G core network, three sources close to the matter said, the clearest sign yet Rome is adopting a tougher stance against the Chinese group.

The decision, made at a cabinet meeting late on Thursday, marks the first time Italy has vetoed a supply deal over 5G core networks with Huawei.

Visiting Italy in September, U.S. Secretary of State Mike Pompeo described Chinese mobile telecoms technology as a threat to Italy’s national security.

Huawei strongly rejects the charges, and its Italian unit said it was ready to undergo any scrutiny to show that its technology was safe.

However at Thursday’s meeting, the government used its special vetting powers to block Fastweb, the Italian unit of Swisscom, from implementing a supply deal with the firm in the most sensitive part of its fifth generation mobile network, the sources said.

“The government has vetoed the operation, asking Fastweb to diversify its suppliers,” a senior government source told Reuters.

Fastweb had picked Huawei as the sole supplier for its 5G core network, sources said. Huawei and Fastweb both declined to comment.

A source from the Prime Minister’s office said Rome also wants to evaluate whether Huawei can play a role in 5G core networks.

While some U.S. allies, such as Britain, have announced bans on Huawei equipment in future telecoms infrastructure, Italy has so far declined to do so.

However, government and industry sources say Rome is de facto adopting a more marked pro-U.S. line on 5G deals.

Italy raised hackles in Washington last year when it became the first major Western economy to join China’s international infrastructure project, the Belt and Road Initiative.

The tie-up has so far yielded little economic gain and the government has recently opted for increasingly stringent prescriptions over Chinese 5G suppliers, which is forcing companies to be more cautious about dealing with Huawei.

Measures imposed by the government on firms using Huawei equipment on their 5G network include restrictions on remote interventions to fix technical glitches and an extremely high security threshold, two industry sources have said.

Italy’s biggest phone group Telecom Italia (TIM) in July left Huawei out of an invitation to tender for a contract to supply 5G equipment for its core network, where sensitive data are processed.

Telecommunications companies operating in Italy have introduced get-out clauses in 5G deals with Huawei, allowing them to withdraw should Rome ask for costly requirements in exchange for its green light, industry sources said.

### Solvency---AT: Say No---Latvia

#### Latvia’s on the fence now BUT US pressure ensures say yes.

Una Aleksandra Bērziņa-Čerenkova 21, the Head of Riga Stradins University China Studies Center and the Head of the New Silk Road program at the Latvian Institute of International Affairs, January 2021, "Latvia: no place for ambiguity," *Huawei in Central and Eastern Europe: Trends and Forecast*, pp. 13-14, <https://chinaobservers.eu/wp-content/uploads/2021/01/briefing-paper_huawei_A4_03_web-1.pdf>, RMax

Latvia became the second among the Baltic countries, after Estonia, to sign the Joint Declaration on 5G Security with the US22 on February 27, 2020, ending a period of political ambiguity on the issue. The text of the document remains classified. However the Latvian public broadcaster has reported that according to its sources the text speaks of Latvia’s commitment to examine “whether a 5G technology supplier isn’t creating security risks”.23 The Minister of Foreign Affairs implicitly reaffirmed the most probable exclusion of Huawei: “These companies have to take into account that there will be certain questions at the moment when they’ll want to cooperate with state structures, especially with those state structures that deal with security, foreign policy and issues of such level.”24

Although the joint declaration, as in other cases, is a non-binding one, under the current circumstances, the entry and development of Huawei in the segment of 5G networks can be characterized as “never say never, but extremely complicated”.25 Interestingly, unlike in North Macedonia or Cyprus, the signing of the declaration was not followed by a reaction or statement of the Embassy of the People’s Republic of China.

A strong signal that Latvia plans to rely on Northern European 5G infrastructure providers also came from the Ministry of Defense, as the “first 5G military test site in Europe”26 was launched at the Ādaži base by the mobile network operator Latvijas Mobilais Telefons (LMT) on November 13, 2020. LMT, the majority stake in which is owned by the state of Latvia, and the minority stake by the Swedish-Finnish TeliaSonera, is cooperating with Nokia on 5G. The 5G military test site featured only 5G routers locally produced by the Latvian company MicroTik.

The remaining two network operators aside from LMT (namely Tele2 and Bite) followed the ambiguous approach longer, but it is also coming to an end. Bite Latvija, owned by the US private equity investment fund Providence Equity Partners LLC27 through Bite Lietuva, had signed an MoU on cooperation in 5G networks with Huawei in 2018, and had been consistently voicing a pro-Huawei position: “Latvian mobile phone operator Bite Latvija will not suspend its partnership with the company and will go forward with its plans to introduce a 5G network with the help of Huawei.”28 However, upon the signing of the Joint Declaration, Bite’s messaging became less assured, claiming that even though “it’s still unclear which company’s technology will be used”, Bite is “developing a 5G network in cooperation with (..) Tele2, (…) Tele2 is also developing a parallel 5G network using Nokia infrastructure”.29

As in similar cases across Europe, one cannot say with full certainty that Huawei will be excluded from the rollout of the 5G network in Latvia. Still, the local mobile network operators (MNOs) are becoming increasingly aware of the risks the cooperation with Huawei will bring, making Huawei participation in 5G network installation in Latvia very unlikely. Certainly, the final decision of Bite Latvia is a to watch aspect, as currently it is the only mobile network operator that had planned to cooperate with Huawei. Although the MNOs are generally reluctant to commit to the exclusion of Huawei, and the issue is mostly promoted by the defense-oriented government actors, the leeway of mobile network operators is very limited, because the push towards the exclusion of Huawei ultimately comes from Latvia’s primary security guarantor – the United States.

### Solvency---AT: Say No---Lithuania

#### Lithuania says yes.

Deeba Ahmed 21, reporter for Hackread.com, 9/24/2021, "Lithuania wants users to dump Chinese phones citing data collection," <https://www.hackread.com/lithuania-dump-chinese-smartphones-data-collection/>, RMax

Lithuania’s Defense Ministry has released a warning, urging consumers to get rid of their Chinese phones and not to buy new ones.

This warning comes in response to Lithuanian cybersecurity researchers identifying several security flaws and censorship-related loopholes in certain Chinese-made smartphones.

Hackread.com has learned that researchers tested 5G mobiles from different Chinese mobile makers, including Huawei, Xiaomi, and OnePlus 8T.

Four Major Cybersecurity Risks Discovered

Lithuania’s National Cyber Security Center (NCSC) revealed that four major cybersecurity flaws were identified in smartphones made by Xiaomi and Huawei. Two of the flaws were related to pre-installed applications, and one was involved in private data leakage.

Huawei P40, according to the report, is responsible for putting users at risk of cyber-security breaches. The report revealed that the official Huawei application store called AppGallery is directing users to third-party stores. Some of the apps uploaded at the store were declared malicious or infected with viruses after these were scanned through anti-virus programs.

After the NCSC’s report, the Defense Deputy Minister of Lithuania, Margiris Abukevicius, released this statement.

“Our recommendation is to not buy new Chinese phones, and to get rid of those already purchased as fast as reasonably possible.”

### Solvency---AT: Say No---Luxembourg

#### Luxembourg says yes.

Anne Morris 20, contributing editor for Light Reading, 12/15/2020, "Proximus dumps Huawei in Luxembourg too," Light Reading, <https://www.lightreading.com/5g/proximus-dumps-huawei-in-luxembourg-too/d/d-id/766126>, RMax

Yet another European mobile network has decided to drop Huawei in favor of a less complicated relationship with a more local vendor.

Proximus, [which has already turned to Ericsson and Nokia](https://www.lightreading.com/5g/belgian-telcos-drop-huawei-for-nokia/d/d-id/764525) in its primary market of Belgium, has now also picked Finland-based Nokia for its 5G network in neighboring Luxembourg.

Under a seven-year deal for the Luxembourg network, Nokia said it will supply its AirScale Single RAN (S-RAN) portfolio for both indoor and outdoor coverage, including 5G RAN, AirScale basestations and Nokia AirScale radio access products.

According to Strand Consult, Proximus was previously 100% reliant on equipment from Huawei for its 4G radio access networks (RAN) in Belgium and Luxembourg.

In the Grand Duchy of Luxembourg, Nokia indicated that it will "replace the incumbent radio vendor in the deal with deployment expected to commence next year."

Orange Luxembourg, also said by Strand Consult to be fully reliant on Huawei equipment for its 4G RAN, has already chosen Nokia for its 5G network. Post Luxembourg, which has not previously used China-based vendors, has retained Sweden-based Ericsson for 5G.

Although the Luxembourg government does not appear to have banned Huawei from 5G networks, it has clearly been keeping a close eye on the geopolitical situation and the responses of its European neighbors.

According to a [report](https://today.rtl.lu/news/luxembourg/a/1559647.html) by RTL Luxembourg from August 2020, Prime Minister Xavier Bettel, also Minister of Communications, explained that according to Luxembourg law, operators in the Grand Duchy are obliged to ensure the security of their networks.

It would seem that the local operators are taking "geostrategic sensitivity" into account in their selection of vendors, as Bettel suggested they should do.

### Solvency---AT: Say No---Montenegro

#### Montenegro says yes.

Vaughan O'Grady 22, reporter for Developing Telecoms, 3/8/2022, "Montenegro’s Crnogorski Telekom launches 5G using DSS," <https://developingtelecoms.com/telecom-technology/wireless-networks/13082-montenegro-s-crnogorski-telekom-launches-5g-using-dss.html>, RMax

From the start of this week, the users of Crnogorski Telekom in the Montenegrin capital Podgorica have had access to a 5G network in a number of locations, making the company the first operator in Montenegro to put a 5G network into commercial operation.

The operator says that 5G is available to all users, regardless of the package they subscribe to, as long as they have a suitable device and are in the area covered by the signal.

It’s early days yet of course. The company points out that the gradual extension of 5G coverage will follow until the first in a series of goals is achieved: full coverage of the capital with the new generation network. At the moment, the emphasis is on increasing the capacity of the network and reducing latency.

The estimate is that by the end of May most important areas in Podgorica will be covered, and by the beginning of summer important areas on the coast will have coverage, allowing tourist traffic access to 5G.

The 5G network in Podgorica is based on dynamic spectrum sharing (DSS) implemented by Telekom in partnership with Ericsson Nikola Tesla. This allows existing infrastructure and 4G spectrum to be used.

As for future 5G spectrum availability, spectrum auctions took place in late December. Licences obtained during the auctions are valid between 21 April 2022 and 1 September 2031. 5G mobile networks are expected to be introduced by the end of 2022. It is not clear when they will cover the entirety of Montenegro's territory of 13,812 square kilometres and its 620,739 population.

### Solvency---AT: Say No---Netherlands

#### The Netherlands dislike Huawei.

Reuters 20 – Reuters Staff, 10/15/2020, "Dutch telecom KPN picks Ericsson over Huawei for 5G network," U.S., <https://www.reuters.com/article/us-kpn-5g-ericsson/dutch-telecom-kpn-picks-ericsson-over-huawei-for-5g-network-idUSKBN2700UW>, RMax

AMSTERDAM (Reuters) - KPN has chosen Sweden’s Ericsson to build core elements of its new 5G mobile network following a decision last year not to select China’s Huawei, the Dutch telecoms company said on Thursday.

Huawei is effectively banned in the United States and Washington had expressed fears that if KPN’s 5G backbone contained Huawei equipment it would be vulnerable to spying by the Chinese state.

Huawei, the world’s biggest telecoms equipment and smartphone vendor, has denied U.S. allegations that it is ultimately answerable to the Chinese government and is therefore a security risk.

KPN said in April 2019 that it would select a Western supplier to build its core 5G mobile network, making it one of the first European operators to eliminate Huawei.

In its statement on Thursday, KPN said it “will collaborate with Ericsson” for the implementation of its core 5G technology.

No financial details of the deal with Ericsson were disclosed.

### Solvency---AT: Say No---North Macedonia

#### North Macedonia says yes.

Joe O’Halloran 21, reporter for Computer Weekly, 8/1/2021, "A1 selects Nokia, Ericsson tech for service roll-outs across middle Europe," <https://www.computerweekly.com/news/252505681/A1-selects-Nokia-Ericsson-tech-for-service-rollouts-across-middle-Europe>, RMax

A1 Telekom Austria Group has chosen Scandinavian network equipment suppliers Nokia and Ericsson as partners in the roll-out of 5G networks in the markets of Bulgaria, Croatia, Serbia and Slovenia.

A1 supplies digital services and communications systems in Central and Eastern Europe with about 25 million customers, currently operating in seven countries – Austria, Bulgaria, Croatia, Belarus, Slovenia, North Macedonia and Serbia.

Nokia and Ericsson are already longstanding strategic partners for the operator. By selecting them, A1 Telekom Austria Group took a decision to evolve its networks and services, said Alexander Kuchar, director group technology and future services. “We are demonstrating a strong commitment to providing the best user experience in terms of communications and entertainment services on a high-class and secure infrastructure to our B2C and B2B customers,” he said. “At the same time, we are taking a strong stand on virtualisation, automation and simplification of our network architecture.”

### Solvency---AT: Say No---Norway

#### Norway is phasing out Huawei

Victoria Klesty 19, journalist for Reuters in Oslo, 12/13/2019, "Norway's Telenor picks Ericsson for 5G, abandoning Huawei," U.S., <https://www.reuters.com/article/us-telenor-ericsson-huawei-tech/norways-telenor-picks-ericsson-for-5g-abandoning-huawei-idUSKBN1YH0RM>, RMax

OSLO (Reuters) - Telenor has picked Sweden’s Ericsson as the key technology provider for its fifth-generation (5G) telecoms network in Norway, it said on Friday, gradually removing China’s Huawei [HWT.UL] after a decade of collaboration over 4G.

Fearing high-tech espionage, and battling with China over trade, the United States has pushed NATO allies such as Norway to exclude Huawei from lucrative 5G deals, and Norwegian security services also warned against the firm.

“The 5G era is here. This will be the one technology that will most transform our society in the next decade,” Telenor Chief Executive Sigve Brekke tweeted as he announced that Ericsson will build the 5G radio access network (RAN).

He said Telenor had carried out an “extensive” security evaluation as well as considering factors such as technical quality, innovation and modernisation of the network.

“Based on the comprehensive and holistic evaluation, we have decided to introduce a new partner for this important technology shift in Norway,” he added.

### Solvency---AT: Say No---Poland

#### Poland wants to cooperate with the US.

Alicja Bachulska 21, China analyst at Asia Research Center, War Studies University in Warsaw, Poland, Ph.D. candidate at the Polish Academy of Sciences’ Graduate School for Social Research, January 2021, " Poland: hardening stance," *Huawei in Central and Eastern Europe: Trends and Forecast*, pp. 11-12, <https://chinaobservers.eu/wp-content/uploads/2021/01/briefing-paper_huawei_A4_03_web-1.pdf>, RMax

These events have accelerated Poland’s domestic debate on the role of Huawei in constructing the country’s 5G networks. Simultaneously, growing tensions between China and the US have also affected Warsaw’s perception of threat vis-à-vis Beijing. As the US remains Poland’s key ally in the post-Cold War order, Sino-American strategic rivalry has resulted in Warsaw’s growing skepticism towards unconditional cooperation with Beijing.

During the visit of the US vice president Mike Pence to Poland in September 2019, the two countries signed the US-Poland Joint Declaration on 5G.17 The Polish prime minister Mateusz Morawiecki has also promoted the notion of “European 5G realism”, which in practice means more awareness of risks stemming from technological cooperation with actors from non-democratic states.18

Currently, the most important legal tool that could result in Huawei’s ban in Poland is a draft amendment to the existing cybersecurity law published on September 7, 202019. Some of its provisions suggest that vendors categorized as high-risk would be banned from the Polish market. ICT providers will supposedly be assessed based on a number of categories, some of them indirectly pointing at Huawei. For example, firms from countries outside of the EU might undergo greater scrutiny for political and security reasons. The new law is supposed to come into force by December 21, 2020. At the time of writing, however, the ultimate form of the amendment remains unclear.

In the nearest future, Poland will most probably witness a growing trend towards diversification of telecommunications services providers stemming from both practical and political considerations.

#### Poland says yes.

Laurens Cerulus 20, reporter for POLITICO, 2/3/2020, "Poland wants to go beyond EU on 5G security, says minister," POLITICO, https://www.politico.eu/article/poland-wants-to-go-beyond-5g-security-toolbox-restrictions/, RMax

Poland plans to restrict "high-risk" 5G telecom vendors in ways that go beyond a series of security controls proposed by the European Union, a minister told POLITICO.

The EU last week spelled out a range of options for countries to secure their future networks amid a transatlantic debate about 5G security and Chinese vendors Huawei and ZTE.

But Poland, a close ally of the United States, will introduce tougher controls that would "limit the use of [telecom equipment] vendors who are suspicious or who are not necessarily trustworthy, or who do not stick to the security standards," Digital Minister Marek Zagórski said during an interview in Brussels.

Poland wants to "become independent from one vendor," added the minister, who is a member of the ruling Law and Justice (PiS) party. Local telecom operators procured Huawei equipment for their rollout of previous generations of internet networks, but the government has since turned skeptical of relying on Chinese kit.

#### They’re fearful of 5G insecurity.

Reuters 20 – Reuters Staff, 9/9/2020, "Huawei fears it may be excluded from Poland's 5G network," U.S., <https://www.reuters.com/article/us-poland-5g-huawei/huawei-fears-it-may-be-excluded-from-polands-5g-network-idUSKBN2602BY>, RMax

WARSAW (Reuters) - Poland’s planned criteria for assessing the risk of telecoms equipment providers are political and may be aimed at excluding Huawei [HWT.UL] from developing the country’s 5G network, the Chinese company said on Wednesday.

The United States says Huawei’s equipment could be used by the China for spying - an allegation denied by Huawei and Beijing - and has pressed its allies to ban the company.

On Tuesday, Poland published a draft cybersecurity law, giving interested parties 14 days to comment.

### Solvency---AT: Say No---Portugal

#### Portugal says yes.

Natasha Donn 20, reporter for Portugal Resident, 2/6/2020, "Limits on Huawei in Portugal’s developing 5G network “expected today”," Portugal Resident, <https://www.portugalresident.com/limits-on-huawei-in-portugals-developing-5g-network-expected-today/>, RMax

Limits on the extent to which Chinese telecommunications giant Huawei will be involved in Portugal’s developing 5G network are expected to be announced today, writes Expresso.

The decision will be taken at the weekly ‘council of ministers’ and follows advice from Brussels about reducing exposure to “high risk” suppliers.

Brussels’ warning to all member states essentially focused on the advantages of using “various suppliers” so that no country found itself “dependent” on one alone.

Explain reports, this would almost certainly affect “the scale and depth of the use of Huawei technology in the nation’s future 5G network” as the company is one of the technological partners of national operators Altice and NOS.

Intriguing in this story is the fact that when US secretary of state Mike Pompeo visited Lisbon in January, news stories claimed Portugal had rebuffed US concerns over 5G business with Huawei (click here).

Now, reports are referring to comments made by secretary of state for communications Alberto Souto Miranda last spring, suggesting Portugal was likely to follow Germany’s lead in how to deal with the situation.

Said Mr Miranda, Germany isn’t setting out to ‘banish’ any particular suppliers. Instead it has created a set of security measures through which companies must pass in order for the use of their equipment to qualify.

Today’s developments are expected as the telecoms market awaits information on the imminent 5G ‘auction’, to be held sometime in April.

The idea, says Jornal Económico, is for the national ‘roll-out’ of 5G to begin in June.

### Solvency---AT: Say No---Germany

#### Germany opposes Huawei---recent events prove.

Andreas Rinke 20, journalist for Reuters in Berlin, 9/30/2020, "Germany moves to toughen Huawei oversight: sources," U.S., <https://www.reuters.com/article/us-germany-huawei/germany-moves-to-toughen-huawei-oversight-sources-idUSKBN26L16Q>, RMax

BERLIN (Reuters) - The German government is planning tougher oversight of telecoms network vendors that, while stopping short of a ban on Huawei [HWT.UL], will make it harder for the Chinese company to keep a foothold in Europe’s largest market.

Three coalition and government sources said on Wednesday that an agreement had been reached in principle to extend scrutiny of a vendor’s governance and technology to Radio Access Networks (RAN) powering next-generation 5G services, in addition to the more sensitive core.

The Handelsblatt daily reported earlier that, after two years of wrangling, Chancellor Angela Merkel’s coalition had agreed on a formula for how to handle so-called high-risk vendors in a proposed IT security law.

Merkel’s spokesman, Steffen Seibert, declined to comment on the Handelsblatt story, telling a government news conference that the same security standards would apply to all vendors. The interior and economy ministries, both run by Merkel allies, said discussions on the legislation were continuing.

European governments have been reviewing market leader Huawei’s role in the building of their networks following pressure from the United States, which says it poses a security threat because, among other concerns, Chinese companies and citizens must by law aid the state in intelligence gathering.

Restricting Huawei is the right approach, a senior U.S. official said, urging Berlin to support its NATO allies by removing Chinese technology from its next-generation networks.

“We are seeing things moving in the right direction in Germany ... There is really no future with Huawei,” said Keith Krach, the U.S. undersecretary of state for economic affairs who has visited Berlin and Brussels in recent days.

### Solvency---AT: Say No---Turkey

#### Turkey’s openness to Open RAN proves cooperation is viable.

Thomas Duesterberg 21, senior fellow at Hudson Institute, 3/17/2021, "U.S. Efforts To Counter Huawei 5G Dominance Making Progress: Open RAN Playing Growing Role," Forbes, <https://www.forbes.com/sites/thomasduesterberg/2021/03/17/us-efforts-to-counter-huawei-5g-dominance-making-progress-open-ran-playing-growing-role/?sh=7f449f0b655e>, RMax

Two of the three major Indian telecom operators, Reliance Jio and Bharti Airtel, have developed Open RAN network technology, working with U.S. and Japanese equipment makers and system integrators. In that underdeveloped market which features over a billion, mostly low-cost, mobile users, the Open RAN technology will allow faster and much less expensive deployment of high speed 5G than the traditional hardware systems offered by Ericsson, Nokia, Samsung and even Huawei. U.S. system integration firm Parallel Wireless estimates that Open RAN solutions, although needing some technological advances in energy efficiency to reach their full potential, could result in cutting total operating costs by 30-50%. In Turkey, telecom giant Turk Telecom is working on an Open RAN system, and Vodafone Turkey has already deployed such a network which is backwardly integrated with legacy 2-3-4G systems.

In the United States the three major mobile operating companies are all members of the Open RAN Policy Coalition and the international O-RAN ALLIANCE. All are developing products utilizing the new technology. The case study that likely will determine the economic viability of the new technology in the U.S. market is DISH network. The new operator is committed (under an [agreement with the U.S. Department of Justice](https://variety.com/2019/digital/news/doj-tmobile-sprint-merger-dish-sale-1203279763/) to acquire spectrum and other assets from T-Mobile) to field a nationwide 5G network by 2023. It has chosen Open RAN technology for its system and is working with major system integrators Altiostar and Mavenir, and equipment and software makers Red Hat, VMMare, Cisco, and Qualcomm as well as Ericsson and Nokia. DISH plans to do a limited commercial launch by the third quarter of 2021.

Cooperation among allies to realize the potential of alternatives to Huawei also appears to have growing support. In 2021 the EU has surfaced proposals to cooperate on joint technology work with the U.S., including in telecommunications. According to survey data, most nations in Southeast Asia are looking for alternatives to Chinese equipment suppliers. Japan, Australia and the United States are calling on their respective international development agencies to support infrastructure investment alternatives to Chinese firms. Such support could be of material political and economic interest since Japanese and U.S. equipment makers are leaders in this technology.

#### They’re recently cooperated with Ericsson.

Ericsson 21, 6/9/2021, "Türk Telekom and Ericsson sign a new technological business partnership ," No Publication, <https://www.ericsson.com/en/press-releases/5/2021/turk-telekom-and-ericsson-sign-a-new-technological-business-partnership>, RMax

Türk Telekom and Ericsson (NASDAQ:ERIC) have signed an agreement for the deployment of [Ericsson Dynamic Activation](https://www.ericsson.com/en/portfolio/cloud-software--services/automated-network-operations/orchestration/dynamic-activation) (EDA), a provisioning platform for the rapid and automated activation of telecommunications services in mixed network environments. This agreement expands Ericsson’s partnership and market share with Turk Telekom making Ericsson Turk Telekom’s mobile network IT provisioning partner.

### Solvency---AT: Say No---Romania

#### Romania says yes.

Andreea Leonte 21, independent researcher focusing on China and the President of MaEduc, a Romanian NGO active in the field of civic education, January 2021, " Romania: decisive opponent," *Huawei in Central and Eastern Europe: Trends and Forecast*, pp. 9-10, <https://chinaobservers.eu/wp-content/uploads/2021/01/briefing-paper_huawei_A4_03_web-1.pdf>, RMax

Although Huawei has a large presence in Romania in the existing 3G and 4G networks, having close relations with most telecommunications operators, as well as a regional support center in Bucharest, its chances to lead the Romanian 5G rollout are extremely small.

Romania has not yet organized the 5G tender, despite it being initially scheduled to take place last year. The tender was postponed for 2021, as the legislative framework detailing the obligations of future suppliers is still pending. The reason for the delay was that the Romanian government was waiting for the European Commission to enact measures concerning the security of 5G networks in the EU.

Regarding 5G, Romania was the first country to sign a Memorandum of Understanding1 (MoU) with the US, on the occasion of a presidential visit to Washington by Klaus Iohannis, on August 20, 2019. The MoU provided for the rigorous evaluation of all future 5G vendors to determine if they have a transparent ownership structure and ethical corporate practices, as well as if they are subject to the control of a foreign government, outside an independent judicial review. Although this document did not explicitly exclude Huawei from supplying 5G equipment to Romanian telecommunication operators, the company could hardly meet the conditions named in the MoU. At the same time, the MoU should be interpreted in conjunction with the US Federal Register of Entities,2 which lists all entities believed to pose serious national security/foreign policy threats. Huawei was added to the list on May 15, 2020, together with other 114 of its overseas-related affiliates.3 Since Romania has pledged to have a close cooperation with the US on 5G security, the chances that Huawei could win the 5G bid are remote.

After his visit to the White House, the Romanian president Iohannis discussed the MoU with Romania’s National Defense Council (CSAT) regarding how to transpose it into national law. A year later, on August 4, 2020, a first draft law4 was published on the website of the Ministry of Transport, Infrastructure and Telecommunications.

The draft law states that all manufacturers of technologies, equipment and software programs, which are intended for the use in the national 5G networks (as well as in the information and communication infrastructures of national interest), should obtain an authorization, granted by decision of the prime minister. However, the authorization is conditioned by a favorable opinion from the CSAT, after performing a thorough assessment of the risks, threats and vulnerabilities to the national security and/or national defense of the equipment manufacturer. The authorization may be withdrawn following the same procedure.

The draft law also mandates the National Communications Authority (ANCOM) to request detailed information about the technologies, equipment, and software used in 5G networks, as well as their manufacturer, the degree of outsourcing to third parties of certain activities related to the management of electronic communications networks provided. Failure to provide this information can result in heavy fines. Moreover, the law sets out measures for phasing out the technologies, equipment and software currently in use from noncompliant providers.

On September 11, 2020, Huawei contested Romania’s new 5G security rules in a letter to Margrethe Vestager, the European Commission’s executive vice-president responsible for EU digital policies.5 The letter was sent by Huawei’s Belgian subsidiary, which argued that the new rules follow biased and ambiguous criteria, which are in violation of EU law. The CEO of Huawei Romania also opined that the law was introduced in public debate for too short a time, only between August 4 and 17, thus the telecom industry specialists could not assess its impact.6 The Commission, however, dismissed these allegations, noting that member states may adopt national cyber security rules through European telecoms legislation.

In November 2020, Romania’s prime minister Ludovic Orban7 explicitly excluded a partnership with the company in an interview for Radio Europa Libera8 – a direct consequence of Romania’s strategic partnership with the US on security issues. We can, thus, conclude that Huawei’s prospects for participating in the construction of the 5G infrastructure in Romania are slim.

### Solvency---AT: Say No---Slovakia

#### Slovakia prefers 5G security.

Matej Šimalčík 21, Executive Director at Central European Institute of Asian Studies (CEIAS) in Bratislava, Slovakia, January 2021, " Slovakia: undecided latecomer," *Huawei in Central and Eastern Europe: Trends and Forecast*, pp. 19-20, <https://chinaobservers.eu/wp-content/uploads/2021/01/briefing-paper_huawei_A4_03_web-1.pdf>, RMax

Nevertheless, only a third of Slovak population favor Chinese vendors as suppliers of the network equipment, ranking far behind European and Japanese vendors.66 Similarly, over half of the population thinks that cybersecurity should be a priority for Slovak policy towards China.67

Thus, it should come as no surprise that Huawei has gone on a PR counter-offensive to soften the blow of a harder government stance.68 Despite this counteroffensive, it seems unlikely Huawei will be able to sway the opinion of key policy makers. Indeed, the chairman of the parliamentary Defense and Security Committee stated that the National Council is wary of security risks posed by Chinese tech companies.69 Recognition of these risks was translated into the new Security Strategy of the Slovak Republic, which was adopted by the government in December 2020. The government claimed that it will ensure that construction of critical communication and data transfer infrastructure is built using only equipment and technologies that don’t pose security risks and originate from Slovakia’s partners and allies.70

### Solvency---AT: Say No---Slovenia

#### Slovenia says yes.

Joe O’Halloran 21, reporter for Computer Weekly, 8/1/2021, "A1 selects Nokia, Ericsson tech for service roll-outs across middle Europe," <https://www.computerweekly.com/news/252505681/A1-selects-Nokia-Ericsson-tech-for-service-rollouts-across-middle-Europe>, RMax

A1 Telekom Austria Group has chosen Scandinavian network equipment suppliers Nokia and Ericsson as partners in the roll-out of 5G networks in the markets of Bulgaria, Croatia, Serbia and Slovenia.

A1 supplies digital services and communications systems in Central and Eastern Europe with about 25 million customers, currently operating in seven countries – Austria, Bulgaria, Croatia, Belarus, Slovenia, North Macedonia and Serbia.

Nokia and Ericsson are already longstanding strategic partners for the operator. By selecting them, A1 Telekom Austria Group took a decision to evolve its networks and services, said Alexander Kuchar, director group technology and future services. “We are demonstrating a strong commitment to providing the best user experience in terms of communications and entertainment services on a high-class and secure infrastructure to our B2C and B2B customers,” he said. “At the same time, we are taking a strong stand on virtualisation, automation and simplification of our network architecture.”

In Bulgaria, Nokia is building the radio network and Ericsson the core network; in Croatia, Ericsson is responsible for both radio and core network; in Serbia and Slovenia, Nokia is responsible for both radio and packet core network. In Austria, it was announced in spring 2019 that Nokia would be the chosen partner in the 5G roll-out of both radio and core network domains.

### Solvency---AT: Say No---Spain

#### Spain is phasing out Huawei.

Inti Landauro 21, journalist for Reuters in Madrid, 12/27/2021, "Telefonica buys Ericsson 5G equipment to replace some Huawei gear," <https://www.reuters.com/markets/deals/telefonica-buys-ericsson-5g-equipment-replace-some-huawei-gear-2021-12-27/>, RMax

MADRID, Dec 27 (Reuters) - Telefonica (TEF.MC) has bought 5G network equipment from Swedish manufacturer Ericsson (ERICb.ST) to replace some of the Huawei gear it has rolled out in Spain, a source at the Spanish firm said on Monday, confirming a report in Expansion newspaper.

The replacement of the next-generation mobile network equipment is part of Telefonica's strategy announced in 2019 to diversify suppliers, according to the source.

### Solvency---AT: Say No---United Kingdom

#### The UK says yes.

Howard Solomon 21, reporter for IT World Canada, 7/21/2021, "Huawei network gear again fails to meet cybersecurity quality, says UK board," IT World Canada - Information Technology news on products, services and issues for CIOs, IT managers and network admins, <https://www.itworldcanada.com/article/huawei-network-gear-again-fails-to-meet-cybersecurity-quality-says-uk-board/456099>, RMax

Some of Huawei’s telecom equipment has again failed to meet the cybersecurity quality standards of a United Kingdom agency that examines potential risks of the company’s products in telecom networks.

There was “no overall improvement over the course of 2020 to meet the product software engineering and cybersecurity quality” expected by the U.K.’s National Cyber Security Centre (NCSC), according to the annual report released Tuesday by the Huawei Cyber Security Evaluation Centre’s Oversight Board.

The report doesn’t say whether backdoors have been found in the software code, but previous reports have said the problems are in code quality not malicious activity.

However, it also says the engineering and cybersecurity quality issues are part of long-term, systemic defects in Huawei’s software engineering and cybersecurity competence.

The proposed U.K. Telecommunications (Security) Bill, now close to Parliamentary approval, should provide a framework for addressing the strategic risks in Huawei and other manufacturers’ products differently, the report says. Briefly, the bill would give the government new powers to boost the security standards of the U.K.’s telecommunication networks, including banning risky equipment suppliers and setting technical standards to be met.

The NCSC anticipates that the new security obligations in the bill will result in improvements in the security of all vendor equipment, the report adds.

Last year the U.K. banned telecom companies there from installing Huawei equipment on their 5G wireless networks.

# Case---Commercial

## Mechanics

### Commercial---2AC

#### **NATO key—5G poses substantive threats to collective defense and deterrence against China—NATO’s adaptive capacity is vital**

Julia Pallanch and Amy Yanan Zhang, 2021; Pallanch, program assistant of the Asia Program at the German Marshall Fund of the United States, M.A. in Modern East Asian Studies from University Duisburg-Essen, specializing on Chinese Foreign Policy and EU-China relations; Zhang, Master de Droit (en relations internationales), M.S. en sécurité internationale; “China, 5G, and NATO Security” 10/27/2021, <https://www.gmfus.org/news/china-5g-and-nato-security>//ekc

From the major trifecta of summits around President Joe Biden’s visit to Europe during the summer, it has become clear that China will occupy a central role in the transatlantic relationship in the years ahead.

China now intersects with NATO’s agenda in several ways and occupies a far more entrenched part of the discussion. While NATO is not in a military conflict with China, Beijing remains a key geopolitical competitor to the West. Moreover, the United States sees China as a direct national security threat, and several plausible contingencies could draw the two sides into military confrontation.

The Right Role for NATO

While there are still debates about how far Europe and the United States should be aligned on China, the European NATO members have traditionally assumed part of the U.S. security and defense agenda in exchange for security guarantees. However, China also poses a set of distinctly security risks for Europe, particularly relating to resilience and critical infrastructure and to the considerable dependency of Europe’s digital infrastructure on Chinese technology. The current debate lies in whether NATO is the optimal platform to address those issues, if the EU should take a more active role instead, or if there is an appropriate division of responsibilities between them. For resilience to be the catalyst of closer NATO-EU cooperation, a balance must be found in which the roles of both sides are explicitly defined.

While NATO is adopting a more robust framework in the non-military dimension, it ultimately remains focused mostly on political coordination and consultation, crisis management and collective defense, and interoperability. The EU, on the other hand, has a range of regulatory instruments at its disposal, including the 5G Toolbox and the European Democracy Action Plan, to address some of the wider resilience issues. Future NATO­–EU cooperation should be established on the basis of closer linkages between traditional military-capability planning and resilience requirements, as well as a clear understanding of common ground and shared responsibilities.

Defense of Civilian Telecommunications

Strong, modern telecommunications infrastructure capable of intercepting and withstanding hybrid interference is a prerequisite for NATO to deliver on its key mission of collective defense. Yet, this infrastructure in Europe is largely privately owned, and as such is left exposed to the risk of external interference and susceptible to economic decisions that can neglect national security aspects if not clearly regulated by law. Russia is no longer the only state actor resorting to various types of hybrid tactics on NATO territory: China, too, has been using various sophisticated political and non-military tactics to advance its political and economic influence. In the face of these existing threats, it is imperative for NATO and the EU to delineate their scope of action, especially in instances—such as telecommunications—where the line between civil and military infrastructure is not clearly marked.

Technological dominance ensures not only battlefield supremacy but also supremacy beyond it. Such dominance is contingent on a robust and constantly advancing industrial base that integrates civilian and military innovation, research, and development.

Telecommunications play a central role in the functioning of societies and economies, and provide the basis and future of innovation. These two dimensions are subsequently linked in the race for technological supremacy. Technology has been and will be the key to deterrence and defense. Technological dominance ensures not only battlefield supremacy but also supremacy beyond it. Such dominance is contingent on a robust and constantly advancing industrial base that integrates civilian and military innovation, research, and development. Joint innovation initiatives across the Atlantic are essential to maintain and heighten critical capabilities on and off the battlefield. In the interest of maintaining NATO’s competitive edge and strengthening the alliance’s resilience, new political channels integrating the economic dimensions underpinning elements of security policy, particularly with regards to industrial strategy, need to be established.

Prioritize 5G

Given that cyber threats have long been an area of concern for NATO, 5G networks have naturally become a focus for NATO discussions, even if its defense dimensions have only been slowly put on the agenda. In addition, how data is processed and stored is a key security area that must not become a blind spot. Protecting the public sector and industries, along with ensuring that companies, citizens, and government institutions have the possibility of sending their traffic end-to-end to a non-Chinese network, is at the heart of the matter.

In 5G, for instance, cloud infrastructure will play a significant role. Under Chinese law, the government can request and be granted access to the data of any private company in China, putting at risk all data on a Chinese 5G cloud. To take the example of Belgium, all of its telecommunications infrastructure was previously reliant on Chinese equipment, including mobile communications used by the EU and NATO administrations. Similarly, Chinese equipment today permeates Germany’s networks, meaning that the mobile traffic of all NATO troops based in Germany goes, at some point, through networks reliant on Chinese technology. Deutsche Telekom’s cloud, built and run by Huawei, had the Nuclear Research Center (CERN) in Switzerland as a key reference customer upon its launch. While it is clearly a minimum requirement to have scrutiny in place for networks that fulfill functions for government networks, defense industry, and internal security, networks that fulfill critical functions for society, such as in utilities and pharmaceutical industries, healthcare, banking, or transportation and communication, must likewise not rely on Chinese equipment.

The cost of replacing Chinese telecommunications infrastructure in Europe will not be prohibitive: as operators upgrade from 4G to 5G, all aging equipment will be replaced regardless.

As such, a total ban on new Huawei equipment in Europe could “naturally” take about six years before the installed untrusted base is simply phased out. The question then, is rather one of ensuring a faster transition towards trusted technology on national security grounds, where short-term commercial considerations regarding phaseout times do not determine the pace. Chinese vendors are neither more technologically advanced, nor more competitive than their European counterparts: they simply rely on a system in which the combination of subsidies for homegrown companies operating on global markets and a heavily protected domestic market continue to distort the playing field. The issue is most acute for the smaller operators across Europe, Latin America, and Asia, which have weaker credit scores and thus must resort to Chinese loans unless alternative financing mechanisms are offered. The United States and South Korea are considered leaders in 5G network rollout, yet their infrastructure has been deployed without using any Chinese equipment, instead relying mostly on European technology. One commonly suggested long-term alternative is Open RAN, but, in practice, Chinese presence and influence in its development structures requires a comprehensive risk assessment.

The EU Toolbox for 5G security offers a good framework for initial action, but its non-compulsory nature allows for different interpretation and implementation across EU members, leaving vulnerabilities. One step in the right direction would see the stricter implementation of the toolbox across the EU, but this is only a starting point. Networks connecting critical assets via fiber optics, transport, and undersea cables require the same scrutiny and strict implementation of safeguards. The joint development of toolboxes for these network perimeters could then be envisioned too.

China and NATO

Despite the nuanced language adopted at the NATO summit, the perceived threat to the security interests and democratic principles of the alliance have raised the China issue to the status of a major NATO agenda item. The alliance’s policy towards China will be solidified in the upcoming Strategic Concept, which is expected to be adopted at the next summit. The difficulty then will be for NATO to address the various and diverse security threats at once: hybrid deterrence, disruptive and emerging technologies, and vulnerable critical infrastructure. Given the fast-changing security landscape and the rapid development of technology, its ability to adapt to this new scenario and act effectively on all these fronts will be crucial to NATO’s future.

#### Correcting the lack of a uniform directive in NATO for the 5G race is key to prevent Chinese exploitation of 5G equipment

David A. Andelman, 19; exec. Director of The RedLines Project, BA of Diplomatic History from Harvard, Masters in journalism at Columbia, former domestic and foreign correspondent at the New York Times, Paris correspondent at CBS news, executive editor at Forbes, editor in chief and publisher at the World Policy Journal, board of contributors at USA TODAY, editor emeritus at the World Policy Journal, and current global affairs columnist at CNN; “NATO countries need to stop China from winning the 5G race” April 15th, 2019 https://www.cnn.com/2019/04/15/perspectives/huawei-5g-nato/index.html//ekc

Fears that Huawei and its 5G wireless equipment could be exploited by the Chinese government to spy on other countries have been growing, spurring some countries — like the United States — to ban the company’s products altogether. Huawei denies that any of its products pose a national security risk.

But a recent report from NATO suggests that banning the company’s products would be shortsighted from a strategic standpoint. While measures need to be put in place to ensure Chinese officials aren’t exploiting Huawei’s equipment, rejecting Huawei and its products could prevent many prospective customers in the West from using the company’s state-of-the-art technology to develop their own advanced 5G downstream services.

Indeed, Huawei has managed to position itself on the cutting edge of a number of innovations in recent years — integrating western technology with its own secret sauce. These efforts are only likely to intensify. What’s essential for users in the United States and other countries is that they carefully monitor how every product is operating and how it is being integrated into their systems.

At the same time, NATO’s researchers advise that telecommunications companies in western countries establish viable alternatives to Huawei’s 5G technology. Indeed, Finland’s Nokia and Sweden’s Ericsson are Huawei’s biggest competitors, but they’ve still lagged behind.

There would be severe consequences should the world depend on a single supplier, especially from a nation like China. Allowing Huawei to develop a global supplier monopoly with 5G technology could enable China to quickly leapfrog the West in developing the next generation space-based 6G networks that are already beginning to appear on some drawing boards, at least in academia. Researchers in Finland, for example, are suggesting 6G will make possible such innovations as clothes that can monitor your health in real-time as part of a fully AI-enabled world. And one can only imagine the military capabilities that 6G would provide. It’s clear the competition between China and the United States is only just beginning.

NATO — a collection of 29 distinct nations, each with its own approach to technological development and open vs. closed markets — has not adopted, and seems unlikely to adopt, any uniform approach to Huawei and whatever challenges it might pose. So in addition to encouraging other nations to develop their own 5G technology to compete with Huawei, NATO should adopt a uniform series of responses to threats from external military or strategic challenges. And if Huawei is found to be facilitating Chinese cyber espionage or military operations, these countries should replace Huawei technology with a host of other alternatives — from providers like Nokia, Samsung, Qualcomm and Intel.

Indeed, governments in western nations should provide subsidies for advanced 5G and 6G research to prevent any one player from achieving utter dominance. In January 2018, Canada provided some $40 million to Nokia for research and development of 5G equipment. The NATO Cooperative Cyber Defence Centre of Excellence (CCDCE), author of this report, should use Canada as a model and coordinate NATO-wide public-private partnerships of this sort. Raising its funding to a level that would allow such joint NATO-wide operations would be an important first step.

The arrival of 5G and the anticipation of 6G, with all the extraordinary global advances they hold, will quickly overshadow any latent fears over the misuse or abuse of these new technologies. Nor should any such concerns restrain innovations that are inevitable at every stage in their development. But vigilance is equally appropriate and NATO is itself uniquely positioned to take the leading role here.

### Commercial---Supply Chains---2AC

#### 5G supply chains at risk of exploitation---DoD-NATO assessment of security risks is key.

Pernik ’21 [Piret; October 2021; Research Fellow at the International Centre for Defence and Security, Researcher at the Cooperative Cyber Defence Centre of Excellence, M.A. in International Relations and European Studies from Central European University, M.A. in Sociology from the Tallinn University Estonian Humanitarian Institute; et al.; "Research Report Supply Chain and Network Security for Military 5G Networks," https://ccdcoe.org/uploads/2021/10/Report\_Supply\_Chain\_and\_Network\_Security\_for\_Military\_5G\_Networks.pdf]

5.1. Supply Chain Security and Risk Management

As discussed in the introduction, the supply chain has become a common attack vector for nation states’ cyber espionage and the theft of government and defence sector data.107 Recent large-scale, high-impact supply chain cyberattacks, for example, NotPetya in 2017 and SolarWinds (also known as Solarigate/Sunburst backdoor malware attacks) in 2020, have disrupted public services in many countries, causing huge economic losses. Moreover, cyberattacks have damaged and disabled critical infrastructure and ICT systems. Supply chain attacks can be difficult to trace and manage. Yet they can cause serious second-order effects such as the sabotage or physical destruction of critical infrastructure, or the theft or manipulation of sensitive or classified information.108 This trend will continue in the current decade, and the repercussions for NATO nations’ economic and national security are likely to be severe.

The use of open source software, poor coding practices, insufficient patching, and cyber hygiene; the reliance on commercial-off-the-shelf (COTS) products, systems, and services; and the complexity of global supply chain bring new threats to the military use of 5G technology. The global and distributed nature of product and service supply chains make it difficult to determine how the acquired technology has been developed and deployed. In addition, supply chain risks can also include so-called insider threats.109

Broadly speaking, supply chain security risks concern the reliability, availability, safety, and redundancy of networks, as well as the market diversity of 5G equipment and associated services. Supply chain risks to market diversity constitute a situation where MNOs have limited choice of equipment vendors. This can happen when a single vendor, whose proprietary hardware and software is not interoperable with other vendors’ products, dominates a global market. In this example, a lack of vendor choice can lock a MNO into using equipment from an untrusted vendor, which creates new security risks related to the supply chain. Further examples of cyber supply chain risks include: insertion of counterfeits; unauthorised production; malicious insiders; tampering; theft; insertion of malicious software and hardware (GPS tracking devices, computer chips, etc.); and poor manufacturing and development practices in the cyber supply chain. These risks are realised when threats in the cyber supply chain exploit existing vulnerabilities.110

Supply chain attack vectors can be utilised at any point during the ICT life cycle, from design to maintenance and retirement. Implants (or other vulnerabilities inserted prior to the installation of equipment) can be used to infiltrate government and defence sector data or manipulate hardware and software, computer operating systems, or end user devices and associated services for economic, political, and military purposes.111 For example, the Solarigate/Sunburst supply chain attack, which has been attributed to the Russian government, targeted the software development process; this popular attack vector has frequently been used by Russia, China and other authoritarian countries.112 Software supply chain attacks can also target telecommunications technology, including 5G networks – for example, VNF and software defined networking (SDN) introduce vulnerabilities to the core network, which may be exploited by malicious actors.

The US DoD 5G Strategy prescribes addressing strategic risks and adopting mitigation measures to minimise risks to the supply chain. The strategy prescribes avoidance of the use of 5G technology vendors who are considered untrusted or who have unreliable products.113 Likewise, the Prague Proposals on 5G security (2019) and the Centre for Strategic and International Studies (CSIS) ‘Criteria for Security and Trust in Telecommunications Networks and Services’ (2020) provide further non-technical criteria for national decision-makers to assess risks to determine the trustworthiness of a potential supplier and manufacturers.114 For example, the CSIS criteria include the following aspects: political and governance, business practice assessment, and cybersecurity risk mitigation criteria, and government actions to increase confidence in choosing a supplier.115 The EU assessment and Prague Proposals address many of the same concerns.

In regard to the supply chain risk, the main concerns of the US Cybersecurity and Infrastructure Security Agency (CISA) are counterfeit components (which are more susceptible to cyber-attacks and more likely to fail because of their poor quality) and compromised components. A component may be compromised through interference with the source code repository, the theft of signing keys, or the penetration of distribution sites and channels. The CISA notes that thirdparty suppliers, vendors, and service providers may have weaker security controls and audits than MNOs, which makes compromised components in their supply chain more likely. For example, a MNO may buy the core network system’s management software from a trusted provider; however, it may happen that, unbeknownst to this trusted provider, one of the components it uses in the product is compromised and contains malicious code.116 In an earlier advisory from 2019, the CISA divides 5G security risks into four categories: supply chain, competition and choice, network security, and deployment. According to this simplified approach, supply chain risks include malicious hardware and software and vulnerabilities in the manufacturing of products and their maintenance. The advisory proposes mitigation measures such as adequate standardisation and certification schemes, auditing, and vetting and procurement policies.117

According to a recent survey, large MNOs in the European Union have moved parts of their operations outside the EU countries because of more favourable legislative or business environments. This exacerbates the difficulty of ensuring the reliability, integrity, safety, and security of the supply chain and introduces new vulnerabilities on the top of the existing ones mentioned in this sub-chapter, which can be leveraged by non-EU and non-NATO countries for malicious use.118 In sum, supply chain risk management is a very complex and multifaceted undertaking, requiring building trust relationships and communicating with both internal and external stakeholders.119

It is essential that NATO nations’ governments and militaries have sufficient transparency into the processes, procedures, and practices used by manufacturers of 5G technology and providers of associated services in order to assure the integrity, security, resilience, and privacy, as well as quality, of the acquired products, systems, and services throughout their whole life cycle.120 Hence, militaries must work closely with commercial 5G network providers to jointly assess supply chain and network security risks and add suitable security assurances for military-grade 5G networks. At the time of publication of this Research Report, the Alliance has not begun broad discussions with vendors, MNOs, or other stakeholders on how to achieve comprehensive visibility into the supply chain of 5G networks.

### Commercial---Tech Leadership---2AC

#### Cybersecurity of 5G networks is necessary for democratic digital governance. Transatlantic cooperation through NATO standard-setting is essential to safe and effective regulatory standards.

Chivot ’20 [Eline; 9/10/2020; Senior Policy Analyst at the Center for Data Innovation, M.A. in Political Science and Economics and in Economics and Finance from Sciences Po Lille; Raquel Jorge-Ricart; Fulbright Fellow, at the Elliott School of International Affairs; M.A. in International Relations from the University of Madrid; "The EU’s approach to 5G and the reshaping of transatlantic relations," <https://www.europeanleadershipnetwork.org/commentary/the-eus-approach-to-5g-and-the-reshaping-of-transatlantic-relations/>]

As a security partnership, NATO could potentially serve as a forum for further collaboration on security standards between the EU and the United States. For instance, the Alliance could refine its role in cybersecurity protection, defence, and resilience. The EU is still searching for a common certification strategy to prevent backdoors—hidden entry points for attacking or spying—which may affect 5G hardware. This strategy might help the EU to surpass current national-based approaches, as well as to reshore its internal production capabilities and critical infrastructures’ resilience and could strengthen standards-setting collaboration within NATO regarding the impacts of cybersecurity on 5G networks.

The EU, the United States, and like-minded partners (such as Japan) should renew their dialogue on the implications of state behaviour norms in cyberspace for the protection and resilience of 5G networks. China has become highly active in the multilateral arena by proposing principles regarding the respect for cyber sovereignty and the shaping of new AI-related uses in line with its Belt and Road Initiative and its Digital Silk Road. This may have significant implications on the 5G-driven connectivity of AI applications. A common transatlantic position is therefore sorely needed to tip the balance towards an open, fair, secure, and stable data governance system. Such a “common” position does not refer to similar policies and regulations but would be one through which all partners can cooperate on critical infrastructure connectivity while respecting common values and fundamental rights.

With regards to the digital economy, both allies can mutually reinforce each other’s assets. The EU should work on joint technology initiatives with the US and other partners, as well as pool resources in the many areas that are mutually beneficial. In turn, the EU could use this collaboration as a two-way street, to boost its digital credentials in areas where it has incumbent strengths. The US, which has no major 5G wireless equipment provider, will continue to largely rely on the European companies Ericsson and Nokia but is aiming to accelerate alternatives for the future. These two European firms, which remain the second and third largest suppliers in the race for 5G, are also entering deals with Canada’s largest telecoms companies in order to build their 5G networks.

The importance of 5G systems has taken on a geopolitical dimension. Given its importance as a national security asset and an economic driver, current strategies and principles cannot be limited to national agendas. International stability—security, peace, economy, and respect for human rights—relies on both the effectiveness and long-term readiness of multilateral negotiations. Opening up a deep transatlantic discussion on the role of 5G will be essential to ensure mutually beneficial cooperation. In turn, this will contribute to subsequent ways of dealing with models that might leave Western regulatory standards out of the shaping of a fair and safe technological near-future.

## Answers

### Commercial---AT: 5G Cyber D---2AC

#### 5G adds new dimensions to cybersecurity risks that require NATO defenses.

Giles ’22 [Keir; 7/4/2022; Senior Consulting Fellow at Chatham House, Director of the Conflict Studies Research Centre, Fellow at the National Security Center of Excellence Canada; Kim Hartmann; Cyber and Information Technology Director at the Conflict Studies Research Centre; "Emergence of 5G Networks and Implications for Cyber Conflict," https://doi.org/10.23919/CyCon55549.2022.9810903]

SECTION 4.

Recommendations

As described in Section 2, 5G gives rise to new technical attack vectors, as well as old ones. However, this fact is true for most new technologies, and it is not the reason for this article. The urgency arises due to the processes involved and the effects that the gap between technological implementation and strategic decision may have on the political level. It is important for decision-makers to realize that a basic understanding of the underlying technology is essential and cannot be delegated.

A. Coping with Novel Threats

The technologies used to build our future networks will not only allow us to move forward in application scenario terms but also force us to do so technically and strategically. As an example, ENISA reports that, while it was previously impossible to migrate the workload of a technical component from one service provider outside of the defined legal and policy boundaries of that provider without notice, this threat is now technically feasible. In fact, as georestrictions cannot be enforced on NFVs in 5G, it is possible to move VNF from one location to another undetected.27

Consideration of some of the possible goals of adversary activities and the possible motivation for attacking 5G networks highlights that the threat should not be assessed only in terms of espionage and destruction. Infiltration, control, and strategic and political tactics should also be taken as serious concerns. 5G not only provides us with the capability to accelerate technologically but also provides our adversaries with a new dimension of operational domain. While cyberspace has always been the domain considered most easily attacked remotely and without attribution, 5G takes this statement to a new level. Through the softwarization of our networks, we remove a large portion of the last barrier of what has often been considered the ‘physical security’ of our network backbones. This is a development that cannot be stopped – in fact, reliance on this technology is firmly built into future development plans. But the nature of the threat, especially on the strategic and operational layer, dictates taking precautions now.

B. Exchange Among Professions

As the relevant European institution, ENISA does an excellent job of keeping experts updated and delivering reports on recent developments. However, these reports have a technical depth that will most probably make them incomprehensible to nonspecialists. We strongly encourage lively exchange between technical and strategic personnel. An example of how this can be achieved is to bring together national and international decision-makers and developers in a similar manner as done in agile software development.28 The objective of doing so would be bi-directional: to foster a deeper understanding of the underlying technology at the strategic level and, at the same time, to accelerate the understanding of strategic and political considerations and implications among technical personnel. This requires both groups to have the opportunity to easily and directly exchange their thoughts.

C. Consensus Strategy and Implementation

Furthermore, Western allies must ensure that they not only enforce strategic decisions nationally but also achieve common consensus policies. This will allow limitation in the variation of the technical implementations (which is already considerable) and may reduce incompatibilities. It also provides the chance to better control the gap between policy and implementation. Furthermore, strategies on adequate and secure CI/CD from a strategic view, especially on propagating software updates, must be developed and enforced. Measures must be installed to identify and remove malicious software instances among allies. Ways of ensuring this must be discussed in the context of allied and multinational operations and meeting different nations’ demands collaboratively. Further research and discussion in this field is needed.

D. ‘On-Boarding’

As technical implementation is the practical enforcement of whatever strategic decision is made, awareness among technical personnel of the strategic and political implications of technical decisions must be raised. Additionally, it is reasonable to demand that national institutions place decision-makers in the developer teams of software components that have such a wide impact on national cyber sovereignty.

An example of how this could be done is in the context of agile development by creating a dedicated role within the team. Due to the novelty of the technology and the beginning of an era where cyber sovereignty and the security of states are being placed in the hands of software developers, this role must urgently be defined for exactly this purpose – since it has not been previously required, it does not currently exist. While the exact outline of such a role and the professional skills required still need to be defined, we stress that current practice is inadequate for the described purposes, as it broadens the gap between policy-level stakeholders and the implementation team while not truly ensuring that someone on the team fully understands all technical, political, and strategic decisions.

This approach is feasible if the stakeholder is only interested in the final product outcome but does not need to understand how this product is achieved and if the developers do not care about the political or strategic implications of their development decisions (outside their technical scope). However, when it comes to the development of the backbone of our future networks, the strategic and political knowledge of decision-makers must be integrated into the development process, and strategic and political decision-makers must be aware of how their decisions are being implemented and the implications of the technical decisions being made. If it turns out to be impossible to empower decision-makers to this extent in terms of technical expertise, then consideration should be given to how dedicated professionals with expertise regarding the intersection of technical and political decisions can be educated. How this can be achieved or if there are other ways to solve these difficulties may be a subject for further research.

SECTION 5.

Conclusion

Future network technologies will be critical enablers for economic development and prosperity in NATO member states and among Western allies. But the steady deterioration of relations with key adversaries – and the emergence of new ones – means that any new capability must be carefully assessed to ensure that, along with prosperity, it does not bring a means to severely harm the interests of the state introducing it.

Compared with previous means by which adversaries could attack one or more NATO member states or Western allies, 5G network technology combines a unique, and potentially uniquely damaging, set of attributes. It will be ubiquitous; other key technologies, including critical national infrastructure, will be highly dependent on it; the attack surface is accelerated; and most importantly of all, it will be easily accessible to hostile actors once they establish themselves as contributors to the software backbone. The result is that as well as a radical step forward in telecommunications capability, 5G also risks offering an open door to those who would wish to cause harm.

It is therefore vitally important that planning for further rollout of 5G takes full account of the fact that it is being deployed in a hostile world. An essential element of this is a security mindset that combines geopolitical and technical awareness. This awareness must, in turn, inform a critical assessment of who should and should not be trusted to contribute to the construction of the networks – and, just as vitally, whom they, in turn, enlist as subcontractors. Given the complexity of the software backbone under construction today, it is unlikely that software from contributors found to be questionable can be fully removed at a later date. It is even unlikely that covert operations to compromise network components could be discovered at all. The implication is that NATO states may find themselves operating networks that are partly controlled by foreign nations without them even noticing, until it is too late – for instance, if a hostile power makes political demands while threatening to shut down public communications or network components serving critical infrastructure.

The other vital element of ensuring a secure architecture for 5G is ensuring that technical experts and government-level strategic planners are communicating clearly, effectively, and fully. The challenge of the language gap between technical and policy personnel is hardly a new one – but it becomes vastly more important as network architectures become increasingly incomprehensible to non-experts. Ensuring that both groups are talking to each other in a way that ensures that what is being discussed is implemented, and what is implemented is actually understood with all its strategic and political implications, is another essential safeguard against this vital new technology being used as a weapon against the states adopting it.

### Commercial---AT: EU Solves---2AC

#### EU toolbox is insufficient---alliance wide cooperation is key.

Carisa Nietsche 20, Research Associate in the Transatlantic Security Program at the Center for a New American Security, Martijn Rasser, Senior Fellow at the Center for a New American Security, former CIA officer, 4/30/2020, "Washington’s Anti-Huawei Tactics Need a Reboot In Europe," <https://foreignpolicy.com/2020/04/30/huawei-5g-europe-united-states-china/>, RMax

A coronavirus-induced economic crisis could send Europe bargain-shopping for critical infrastructure—in ways that might be dangerous. Europe’s argument on moving forward with the implementation of Huawei 5G technology against U.S. objections has long centered on cutting costs. The U.S. calls for a ban of the Chinese telecommunications firm’s 5G equipment in European networks have failed to gain traction in most European capitals. Just a handful of countries have echoed U.S. demands for tougher restrictions to supplement the recently released EU toolbox for 5G security, and even fewer have called for an outright ban.

The United States has highlighted the risks that Huawei poses to national security, including the threat of espionage. Given the Chinese Community Party’s effective control of Huawei, there is concern over data integrity. More serious is the potential to debilitate critical infrastructure. 5G will be the backbone of communications and controls needed for power grids, water supplies, and transportation infrastructure. In January, the United Kingdom announced it would allow Huawei equipment on 35 percent of its 5G networks—a decision that could provide top cover for Germany, France, and others to do the same.

Even so, there are bright spots. Estonia and Poland announced stronger restrictions to ensure 5G network security, and some lawmakers, such as Iain Duncan Smith in the United Kingdom and Norbert Röttgen in Germany, remain opposed to Huawei’s inclusion in their networks, leaving hope that a clear-eyed risk assessment will prevail. Recently, technology industry leaders for open radio access networks sent a letter to the U.K. House of Commons Defense Committee urging it to abandon implementation of Huawei technology. Given the uneven response across Europe, where should the United States go from here? It can still sway countries that remain on the fence, but it will need to change tack.

For one, the United States should create a multilateral coalition with like-minded European allies, such as Poland, the Czech Republic, and Estonia, to reboot conversations about Huawei’s role in Europe. A number of European countries perceive Washington as a self-interested messenger and see its fight against Huawei as merely part of a geopolitical game against China. That’s a criticism Washington should answer, and it can emphasize a few key messages to do so.

The coalition should emphasize that the EU toolbox is designed to be a baseline for a common approach, not a final answer. Countries should do their own risk assessments based on their technical capabilities to mitigate risk and secure their networks. The coalition should also dispel the oft-cited myth that there are no viable alternatives to Huawei. The United States, and European adopters of Nokia and Ericsson technology, must tout the value and quality of Nokia and Ericsson kit. For one, the United States should point to the obvious fact that it is building world-class 5G networks using solely Nokia and Ericsson radio access network equipment.

Then there’s the pernicious myth, pushed by Huawei’s public relations team and through Huawei-commissioned reports, that the firm is the undisputed 5G technology leader. While Huawei leads the pack in number of patents, qualitative assessments show that the value of its portfolio is much less than that of its competitors—a classic case of quantity over quality.

Finally, the coalition should also take on the cost argument. While Huawei may provide the cheapest upfront option on the market, countries should examine how Huawei could impose hidden costs on the backend for maintenance and installation, beyond the considerable expense associated with risk mitigation efforts.

The United States should also lead to make new alternatives to Huawei available. A promising approach is to promote open architecture as a way to upend the 5G status quo. Open architecture consists of proprietary software for functions like switching, routing, and firewalls that run on vendor-neutral hardware and standardized interfaces. This would offer Europe a new way to bypass adoption of Huawei in ways that promote vendor diversity, lower cost, and better interoperability. The United States should work with Finland and Sweden to help Nokia and Ericsson, Huawei’s key competitors, transition to this new telecommunications infrastructure model over the next three to five years.

The United States must face the reality of Europe’s strong reliance on China for economic growth. Beijing has been clear that it is willing to retaliate over any country’s decision to ban Huawei from its networks with economic coercion. In December, China’s ambassador to Berlin threatened to torpedo German car sales in China. Beijing directed similar warnings at France. In order to remove the teeth from China’s threats, the United States must show Europe that it is a reliable trade partner, ending its deleterious trade policies toward Europe and threats to levy tariffs on European goods. Further, the United States should expedite U.S.-EU trade agreement negotiations. A robust agreement would help stimulate economic growth and assure Europe that the United States has its back when European countries exclude Huawei from their networks. The United States remains the largest single export destination for EU goods, nearly twice as big as China. Washington should use this economic clout as a bulwark, not a bludgeon.

Finally, the United States should focus more on the norms and values that it shares with its European partners to dissuade them from purchasing Chinese telecommunications equipment. A large part of Huawei’s success in Europe stems from its large-scale lobbying campaign to convince Europe that it is a trustworthy vendor. Huawei launched a campaign highlighting its so-called shared values with Europe. Huawei has likened voting for Huawei 5G with voting for European values. Largely absent from the 5G debate is the fact that China generally, and Huawei specifically, uses 5G technologies as part of its campaign to suppress and isolate Uighurs in Xinjiang, counter protesters in Hong Kong, and exert greater control over the daily lives of all Chinese. Buying Huawei kit subsidizes these actions—ones that go against the core values of the EU itself.

The United States’ one-size-fits-all approach on 5G has not worked in Europe, and it must recalibrate with a tailored, affirmative strategy and abandon the blunt approach of the past two years. This requires Washington to lead in conjunction with key European partners by offering new technological options, strong trade relations, and a united front on shared norms and values. Above all, this means treating Europe as the friend, partner, and ally that it is.

### Commercial---AT: Squo Solves---Huawei---2AC

#### Blocking Huawei is insufficient---NATO must set software security standards.

Giles ’22 [Keir; 7/4/2022; Senior Consulting Fellow at Chatham House, Director of the Conflict Studies Research Centre, Fellow at the National Security Center of Excellence Canada; Kim Hartmann; Cyber and Information Technology Director at the Conflict Studies Research Centre; "Emergence of 5G Networks and Implications for Cyber Conflict," https://doi.org/10.23919/CyCon55549.2022.9810903]

Introduction

Societies will soon be highly dependent on new and highly complex communications technologies currently being rolled out. But these technologies introduce a whole range of new vulnerabilities ripe for exploitation by both state and non-state actors. This paper considers the precautions that must be taken at a state and collaborative level, such as through NATO, in order to avoid worst-case scenarios where adversaries leverage these new vulnerabilities to achieve everything from low-level damage to strategic geopolitical gains.

Many of the application scenarios envisioned in the near future (such as IoT, autonomous driving, and Industry 4.0) will utilize technologies that are increasingly dependent on virtualizations to provide adequate and adaptable network services. These new technologies will determine the digital evolution of the coming years and have in common an increasingly complex underlying technical and strategic configuration. This will make it increasingly hard for decision-makers to estimate the impact their decisions have on the underlying technology and whether political decisions made are technically feasible.

A purely technical approach to the security and protection of critical network infrastructure will be insufficient to keep moving forward securely within the upcoming networks, given recent geopolitical developments. We will discuss how the technology shifts experienced will also impact strategic and political decision-making and how to cope with the implications this has.

5G networks are often perceived as a new networking standard that simply uses a number of new protocols and frequencies. But this is an oversimplified picture of the nature of 5G networks. The underlying structure consists of a mixture of soft- and hardware components whose complexity and orchestration may be difficult even for dedicated experts to grasp fully. This becomes even more evident when security predictions are to be made or when policy regulations are to be implemented technically. Given this level of complexity, it is difficult to lead an adequate, appropriate, and reality-based discussion between technical and non-technical stakeholders. Attempting to do so typically leads to a high level of abstraction and a meta-language that hides any underlying technology. This abstract and veiled discussion does not provide decisionmakers with enough knowledge about the underlying properties to make well-based decisions and – conversely – makes it harder for IT professionals to translate regulatory language into technical implementations, as the demands are technically too unspecific and abstract and sometimes even incompatible with the underlying architecture. This communicative difficulty is already a security threat in its own right and significantly exacerbates already complex technical security concerns.

In October 2019, the EU Commission identified state-sponsored attackers as the main threat to the security of 5G.1 The EU’s risk assessment identified core security requirements that are different for 5G networks. Due to the reliance on software, the types of devices and services connected, and the heavily interconnected nature of 5G networks, there are more entry points for attackers. Nokia’s head of product management security stated that 5G networks have 200 times more attack vectors than their 4G predecessors.2 Network services such as VIMs (virtualized infrastructure managers) have already been identified as crucial assets3 that are expected to be attacked heavily.

The European Union Agency for Cybersecurity (ENISA) report ‘Threat Landscape for 5G Networks’4 describes a list of evolving threats, and multiple experts have published their findings and concerns regarding the security of the underlying technology. While one may assume that the technical community is aware of these threats (although the same assumption may not apply to anyone outside this largely self-contained bubble), what is truly lacking is a discussion on how these threats may impact political decisions and how adversary strategies may utilize this evolving threat landscape to their benefit. The prominent discussion that immediately comes to mind is the exclusion of Huawei from contributing to the development of 5G networks in a range of Western nations. Although this might suggest that there is already adequate discussion on 5G security concerns and their policy implications, closer investigation proves the contrary.

The concerns addressed in the Huawei exclusion were mainly regarding the development of hardware components. From the view of an IT security professional, hardware security flaws are, of course, not to be neglected, but the more serious concern in 5G networks ought to be around the software attack surface. This was not a prominent topic within the public discussion, nor did the discussion lead to clear guidance for how Western nations ought to proceed with Huawei or other software contributors that are considered to be controlled by adversarial state interests.

As 5G, and the already planned 6G, is currently forming the backbone of the networks we use for a multitude of applications, we need to ensure that security aspects are considered adequately and jointly on both the strategic and technical level. Technical flaws in future network backbones resulting from inadequate translation or communication between strategic decision-makers and technical practitioners may render Western nations susceptible to politico-technical blackmail by adversary actors. This is especially the case if the adversary has the technical knowledge and power to abuse these weaknesses and if the adversary is aware of these weaknesses before Western nations are. This is a one-way street – this weakness cannot be used by Western nations for retaliatory offensive measures against such adversaries.

Some of the crucial questions that must be asked among allies are: do we consider security in 5G networks equally, and do we take appropriate actions? Are these actions technically feasible, and do the technical implementations correspond to our strategic plans? Can we agree on equivalent levels of security to be met, and what are our measures to uphold this level of security? Are these measures compatible with each other, especially on the technical level? Or do they induce further security threats? And most fundamentally of all, have plans for networks provided for their protection and resilience against attacks using state-level capabilities and resources?

#### Bans alone are insufficient---only standard setting solves.

Bruce Schneier 20, fellow and lecturer at the John F. Kennedy School of Government at Harvard University, 1/20/2020, "China Isn’t the Only Problem With 5G," Foreign Policy, <https://foreignpolicy.com/2020/01/10/5g-china-backdoor-security-problems-united-states-surveillance/>, RMax

The security risks inherent in Chinese-made 5G networking equipment are easy to understand. Because the companies that make the equipment are subservient to the Chinese government, they could be forced to include backdoors in the hardware or software to give Beijing remote access. Eavesdropping is also a risk, although efforts to listen in would almost certainly be detectable. More insidious is the possibility that Beijing could use its access to degrade or disrupt communications services in the event of a larger geopolitical conflict. Since the internet, especially the “internet of things,” is expected to rely heavily on 5G infrastructure, potential Chinese infiltration is a serious national security threat.

But keeping [untrusted companies](https://www.economist.com/china/2019/08/08/huawei-is-trying-to-solve-a-hard-problem) like Huawei out of Western infrastructure [isn’t enough](https://www.nytimes.com/2019/09/25/opinion/huawei-internet-security.html) to secure 5G. Neither is banning Chinese microchips, software, or programmers. Security vulnerabilities in the standards—the protocols and software for 5G—ensure that vulnerabilities will remain, regardless of who provides the hardware and software. These insecurities are a result of market forces that prioritize costs over security and of governments, including the United States, that want to preserve the option of surveillance in 5G networks. If the United States is serious about tackling the national security threats related to an insecure 5G network, it needs to rethink the extent to which it values corporate profits and government espionage over security.

To be sure, there are significant [security improvements](https://www.5gamericas.org/wp-content/uploads/2019/08/5G-Security-White-Paper-07-26-19-FINAL.pdf) in 5G over 4G—in encryption, authentication, integrity protection, privacy, and network availability. But the enhancements aren’t enough.

This design dramatically increases the points vulnerable to attack.

The 5G security problems are threefold. First, the standards are simply too complex to implement securely. This is true for [all software](https://www.schneier.com/essays/archives/1999/11/a_plea_for_simplicit.html), but the 5G protocols offer particular difficulties. Because of how it is designed, the system blurs the wireless portion of the network connecting phones with base stations and the core portion that routes data around the world. Additionally, much of the network is virtualized, meaning that it will rely on software running on dynamically configurable hardware. This design dramatically increases the points vulnerable to attack, as does the expected massive increase in both things connected to the network and the data flying about it.

Second, there’s so much backward compatibility built into the 5G network that older vulnerabilities remain. 5G is an evolution of the decade-old 4G network, and most networks will mix generations. Without the ability to do a clean break from 4G to 5G, it will simply be impossible to improve security in some areas. Attackers may be able to force 5G systems to use more vulnerable 4G protocols, for example, and 5G networks will [inherit](https://gcn.com/articles/2019/10/21/5g-security.aspx) many existing problems.

Third, the 5G standards committees missed many opportunities to improve security. Many of the new security features in 5G are optional, and network operators can choose not to implement them. The same [happened](https://www.wired.com/story/5g-more-secure-4g-except-when-not/) with 4G; operators even ignored security features defined as mandatory in the standard because implementing them was expensive. But even worse, for 5G, development, performance, cost, and time to market were all prioritized over security, which was treated as an afterthought.

Already problems are being discovered. In November 2019, researchers [published](https://techcrunch.com/2019/11/12/5g-flaws-locations-spoof-alerts/) [vulnerabilities](http://www.documentcloud.org/documents/6544575-5GReasoner.html) that allow 5G users to be tracked in real time, be sent fake emergency alerts, or be disconnected from the 5G network altogether. And this wasn’t the first [reporting](https://i.blackhat.com/USA-19/Wednesday/us-19-Shaik-New-Vulnerabilities-In-5G-Networks-wp.pdf) to [find](https://syssec.kaist.ac.kr/pub/2019/kim_sp_2019.pdf) [issues](https://arxiv.org/abs/1806.10360) in 5G protocols and implementations.

### Commercial---AT: Too Late---2AC

#### America can catch up, especially in 5G.

Monica Alleven 21, 4-1-21, Executive Editor @ Fierce Wireless, https://www.fiercewireless.com/5g/race-to-5g-alive-and-well-for-u-s-china//tyei

What about that ‘race’?

The subject of 5G in China vs. the U.S. came up during a 5G panel last week hosted by Chetan Sharma Consulting, with guests T-Mobile EVP of Advanced & Emerging Technologies John Saw and Intel Corporate Vice President Asha Keddy.

The consulting firm estimates the U.S. had between 30 million to 40 million 5G subscribers at the end of 2020. China had about 180 million 5G subs by the end of 2020 by Sharma’s figures; its numbers are different from China’s because a good portion of its total count is part of “5G package” customers, rather than representing 5G handsets, and Sharma doesn’t count those. Even then, China’s total 5G subscriber count is at least six times larger.

“Never underestimate China’s resolve,” Saw said, adding that it’s important to compare apples to apples. Sure, China’s 600,000+ 5G base stations represent a big number, but its population is a lot larger as well. He suggested considering the number of people served per cell site, which is roughly the same in both situations, and in that sense, they’re neck and neck.

Still, “it’s really not how fast you start, it’s how well you finish,” Saw said. The real question is who will lead in innovation, and he would bet his money on a free market economy of the U.S., where Uber and Airbnb sprang up thanks to a strong LTE network. “I like our chances. I think it’s looking good and looking better for the United States,” he said.

In an interview, Sharma, CEO of the consulting firm, said he sees different dimensions to the 5G race or story. “One dimension doesn’t do justice,” he told Fierce.

Based on penetration, South Korea is ahead and will stay ahead because it’s a smaller country and half of the traffic is already 5G. “From that point of view, it’s clearly way ahead,” he said.

However, if you take the point of view of number of subscribers, China wins, and nobody can catch up to that. In the case of spectrum, the U.S. has emerged the leader in making that available, although it missed a big opportunity in mid-band spectrum for 5G, which other countries seized earlier.

“I think the real test comes from what ecosystem you’re able to build” and how that prospers over a given period of time, Sharma said. That was the case with LTE, where the U.S. was the leader and that fostered the development of the aforementioned companies like Uber and Airbnb.

The real battle is in the enterprise space, and who’s going to build their factories, highways, airports and all sorts of new applications using 5G. “That’s where I think China has an early start,” in the sense that it has been experimenting and getting factories 5G-enabled earlier and faster than the U.S.

“I think the U.S. will start to catch up,” he said, noting the ecosystem that the U.S. boasts includes the likes of Apple, Amazon, Google, Microsoft, Facebook, and the ecosystem around them is vastly superior to that of China.

“From an ecosystem strength point of view, I think the U.S. has a better positioning,” globally, than Chinese companies, he said. China doesn’t have the same global reach for various reasons. “I feel the strength of the U.S. ecosystem will help it stay in the game of 5G,” and in the long run, “I think the U.S. will generate more revenue than China.”

### Commercial---AT: US Won---2AC

#### Current position is weak---security standards are insufficient and non-Huawei companies are capturing market share.

Daniel Gonzales et. al, 2022; senior scientist at RAND (of communications, electronic warfare, cybersecurity, cloud computing, quantum computing, terrorist use of the Internet, and cybersupply chain risk management, examining for policy issues for the DoD and DHS) and a professor at the Pardee RAND Graduate School, PhD in theoretical ohysics from MIT and B.S> in physics from Stanford; “Securing 5G: A Way Forward in the U.S. and China Security Competition” RAND Research Report, ISBN: 978-1-9774-0855-6, <https://www.rand.org/pubs/research_reports/RRA435-4.html//ekc>

The 5G Security Competition

The competitive landscape in U.S. telecommunications has traditionally been viewed through the lenses of economics and technology. The security of U.S. networks was less of a concern because infrastructure suppliers were U.S. or European and presumed trustworthy. Perhaps it was also assumed that U.S. wireless carriers could make U.S. cellular networks secure by modifying or configuring equipment they bought from suppliers. However, 5G networks are now more complex and have many capabilities, settings, and possible configurations. Much of this complexity is reflected in the microchips that can be found in 5G systems. More than 80 percent of all microchips are now made in Asia, and a growing number are made in China. According to industry projections, by 2030, the United States will make less than 10 percent of the world’s microchips, while China and Taiwan together will make more than 40 percent of them (Ip, 2021). Microchips make their way into 5G products in a complex supply chain with many steps and multiple opportunities for microchips to be compromised along the way. Cybersecurity risks might increase significantly when 5G is deployed worldwide unless more-careful attention is paid to the security of the 5G supply chain.

China has used its leading cellular telecommunication company, Huawei, as a means to surreptitiously collect sensitive national security, foreign policy, and IP information around the world. Huawei was caught spying on the African Union, convicted of stealing software code from U.S. companies, indicted by the U.S. Department of Justice for the theft of U.S. company trade secrets, and assessed to be capable of gathering mobile phone user data at scale using its cellular infrastructure equipment deployed in the Netherlands and Belgium. Huawei is subsidized by the Chinese government in many ways, so it can sell its 5G infrastructure products at deep discounts that its Western competitors cannot match. Huawei and ZTE might increase their penetration of the cellular network infrastructure market as 5G is deployed globally, providing China with significant intelligence and illicit economic advantages.

Competition between the United States and China in 5G now involves more than economic markets and technology leadership. Also at stake are the cybersecurity and integrity of next-generation cellular networks. These three dimensions of the 5G competition—economics, technology, and security—are intertwined. The companies that lead in 5G technologies might gain market share, regardless of their security strengths or weaknesses or their trustworthiness, unless cybersecurity and trustworthiness are determined to outweigh technology or economic preferences. Similarly, if a company can sell 5G products at lower prices than competitors can, it will likely gain market share, unless security is made an overriding concern. An untrustworthy company, such as Huawei, can leverage its market position and technology to help China achieve its national security goals and compromise the security of other nations. The security advantage that China might be able to derive from 5G networks will rely on the market position and technological capabilities of its 5G companies.

Table 7.1 summarizes our analysis of the market, technology, and security positions of Chinese and U.S. companies in 5G, including their access to the 5G supply chain. The table indicates where Chinese or U.S. 5G companies have a market or technology advantage (designated by AM or AT , respectively) or a market or technology disadvantage (designated by an DM or DT , respectively). The 5G architecture areas we considered are network infrastructure, mobile devices, mobile device OSs, microchip design, and microchip foundries.

The United States currently has a relatively weak position in two 5G sectors—network infrastructure and microchip foundries—which are at the very top and bottom of the 5G technology stack. In the other 5G sectors, the United States has a relative advantage over or is roughly at parity with China. In the rest of this section, we provide justification for these assessments.

5G Network Infrastructure

China has a global market advantage in the 5G network infrastructure market because the United States relies on foreign suppliers to build the U.S. 5G network and because Chinese companies, Huawei and ZTE, have a significant presence in the global market. Key U.S. 5G infrastructure suppliers are European or Asian companies that might be subject to unfair competition from Chinese companies, outside of the United States and those allied countries that have not banned Huawei equipment in their 5G networks.

Mobile Devices

Chinese and U.S. companies are major players in the mobile device market. Apple is one of the largest and most-profitable companies in the world because of the success of the iPhone. In the highly competitive 5G mobile phone market, Apple and several Chinese mobile phone makers offer a variety of 5G mobile phones. Despite the Huawei blacklisting, other Chinese phone makers have a greater share of the global market than phone makers from other countries.

## Impacts

### Impact---CI---2AC

#### Collapse is likely and existential.

DeNardis ’21 [Dr. Laura and Gordon M. Goldstein; March 3; PhD in Science and Technology Studies from Virginia Tech, Dean of the School of Communication at American University; Adjunct Senior Fellow at the Council on Foreign Relations; Lawfare, “The Real Lesson of the Texas Power Debacle,” https://www.lawfareblog.com/real-lesson-texas-power-debacle]

The infrastructure was essential, ubiquitous and providing basic functionality for everything in daily life from water to heat and transportation. And in an instant it was gone, plunging tens of thousands of residents into a life-threatening crisis. This is, of course, the narrative of the recent debacle in Texas, where a winter storm overwhelmed the state’s electrical grid and brought the state to a near-total blackout. But it should also be interpreted as a preemptive warning of what Americans will face from the next generation of the internet and the new realm of cybersecurity risk it will dramatically amplify.

Both forms of infrastructure—a state-run electrical grid and the 5G and “internet of things” future to which we are rapidly hurtling—share three attributes. First, their construction reflects a lack of imagination about the danger that can quickly coalesce when seemingly remote threat scenarios become real. Second, compounding a lack of analytic imagination is an absence of preparedness. Third, for both the Texas electrical grid and the emerging internet, public policy protections are either meager or completely absent.

In planning for the resilience of its electrical grid, public officials in Texas discounted the potentially devastating disruption that could occur from unpredictable events—whether related to climate change or just a once-a-century anomaly. They also eschewed precautions other states take seriously by allowing for the interconnection of electrical grid supply chains across their borders, ostensibly because of their ideological rejection of federal regulatory oversight governing such arrangements.

As the United States builds out a new national 5G cyber-physical communications network through private service providers, Americans similarly discount the risks—myriad in their diversity and severity—that are orders of magnitude more significant than what Texas confronted recently. More physical things than people are already connected. The super empowered internet of tomorrow, known among some in the field as the “internet of everything,” will exceed by tens of billions of devices the number of connections between individuals simply communicating via social media or digital screens.

This confronts policymakers with an imminent threat: A cyber outage is no longer about losing digital communications but about losing basic societal functioning and even human life. The failure of imagination is to think of the SolarWinds attack on U.S. federal agencies and tech companies as a worst-case scenario. The failure of imagination is to think of cybersecurity through a content-centric lens rather than as possible attacks on the material world. The emergence of internet-connected cardiac devices, digitally dependent cars, and internet-connected agriculture systems portend the stakes of a cyberattack to health care, economic and social functioning, and food security.

The United States should be prepared for, and certainly not be caught by surprise by, such cyberattacks. Yet, the internet of everything is notoriously insecure. Internet-connected physical objects are not necessarily upgradeable. Nor do they come with adequate default security and encryption. The 5G infrastructure that helps connect digital objects has been at the center of debates over Chinese espionage. Industrial cyber-physical systems are based on technical standards that have not been collaboratively vetted for security and interoperability. One of the most infamous cyberattacks—the so-called Mirai botnet that took down major media sites and corporations—hijacked these insecure objects in homes to carry out the assault. The United States is not yet prepared.

Finally, in the race to conceive and deploy effective public policy responses, the U.S. government as a whole is hardly more anticipatory or synthesized in its response to potential calamity than the state of Texas. The focus of U.S. cyber policy remains on information policy issues such as disinformation, manipulation and violent speech rather than securing the digital world that now powers our material day-to-day lives. The Biden administration confronts an enormous challenge in crafting a comprehensive strategy to the cybersecurity risks foreshadowed by the ruinous experience in Texas and its management of vital infrastructure. While the digital world has leapt from two-dimensional to three-dimensional space, cyber policy has not at all jumped from 2D to 3D.

This failure of imagination, preparedness and policy protection must not be America’s cyber future; the stakes are far too high and the costs are far too great. The Texas disaster is a potent illustration of what has always been true: Our digital society and economy are extremely vulnerable and grow more porous and subject to penetration day by day. As digital sensors and cyber control systems become further embedded in physical infrastructure like energy systems, agriculture and transportation, there is no longer a separation between security of the “real” world and security of the online world. They are entangled and increasingly enmeshed—and policy has yet to catch up to either envisioning or mitigating the looming threats the U.S. confronts.

If the energy grid cannot weather a winter storm, how can it be expected to withstand a major cyberattack? What other vital forms of national infrastructure—ranging from water, bridges, highways and roads, and ultimately our day-to-day financial system—are comparably at risk? As Texas dramatizes, it is neither hyperbolic nor exaggerated to assert that our survival could now depend on securing the inevitable cyber-physical future that is accelerating with stunning rapidity.

#### Causes societal collapse and extinction.

Monarch ’20 [Benjamin; April 20; University of Kentucky College of Law, J.D. May 2015, LLM in Energy, Natural Resources, and Environmental Law and Policy from the University of Denver Sturm College of Law, Deputy District Attorney at Colorado Judicial Branch, and Term Member at the Council on Foreign Relations; Journal of Energy & Natural Resources Law; “Black Start: The Risk of Grid Failure from a Cyber Attack and the Policies Needed to Prepare for It,” vol. 38, no. 2]

In the industrial world, when a switch is flipped, we take for granted that it will produce light, boot a computer, illuminate a stadium or activate a power plant. We know, of course, that power losses can and do occur. Many of us have lit candles during a thunderstorm or brought out extra blankets when a blizzard takes down transmission lines. As of this writing, the most populated state in the United States, California, is experiencing rolling blackouts.1 Yet even in prolonged power outages, we expect that electricity will be restored and, consequently, life will return to normal. Perhaps we need ask, however, what if power cannot be restored in a timely manner? Concern is growing that in the not-too-distant future our electricity supply could be irreparably compromised by a cyber attack. The issue when considering a systemic grid failure of this nature is twofold: how did we reach a point where something so critical to routine life now presents an existential threat, and what can we do to mitigate the risk of a catastrophic grid attack?

This article posits that the emergence of cyber attacks on industrial control systems, as a means of war or criminal menace, have reached a level of sophistication capable of crippling those systems. This article argues that a new grid security policy paradigm is required to thwart catastrophic grid failure – a paradigm that recognises the inextricable link between commercial power generation and national security. In section 5, seven policy recommendations are outlined that may, in part, mitigate a future where grid attacks pose existential risk to nations and their citizenry. Those recommendations are: first, develop a comprehensive insurance programme to minimise the financial risk of grid disruption; second, train more cybersecurity professionals with particular expertise in industrial control systems; third, institute a federally mandated information-sharing programme that is centralised under United States Cyber Command; fourth, subsidise and/or incentivise cybersecurity protections for small to mid-size utilities; fifth, provide university grants for grid security research; sixth, integrate new technologies with an eye towards securing the grid; and, lastly, formulate clear rules of engagement for a military response to grid disruption.

The purpose of this article is to provide the reader with an introduction to this complex topic. It is the aim of the author to give orientation to this issue and its many branches in the hope that better understanding will animate further curiosity and, ultimately, positive action on the part of the reader. Although many skilled and earnest people work tirelessly to prevent a grid failure scenario, it is essential that more be added to their ranks each day. Advisors, engineers, regulators, private counsel to power generators, and many others who play roles in electric power production are crucial to this subject. So, while this article provides entrée to the topic of grid security, its long-term objective is to spur action by the entire energy-related community. In the end, no one is immune to consequences of grid failure and, therefore, everyone is responsible, in part, for promoting grid integrity.2 In this regard, lawyers who represent various actors in the energy sector are going to be faced with questions and potential legal risks of a magnitude that they have never experienced before.

1.2. Turning the power back on in a powerless world

‘Black start’, not to be confused with the term ‘blackout’, is the name given to the process of restoring an electric grid to operation without relying on the external electric power transmission network to recover from a total or partial shutdown.3 At first glance, this description is unremarkable, but it implies a disturbing catch-22 – how might one restore power if the entire external transmission network is compromised?

If an electric disruption occurs at a household level, some homes may be equipped with a modest gasoline generator to temporarily restore power. If a hospital loses power, it will almost invariably be resupplied by automatic, industrial-scale generators. These micro considerations hardly give anyone pause; they are hiccups on a stormy night or a snowy day. In other words, their ‘black start’ is a quick and effective process for restoring power. But what happens, at a macro level, when an electric grid supplying power to large portions of the United States goes black, or worse, what happens if all of the United States’ electric grids go down simultaneously?4 In that scenario, how might enough non-grid power be harnessed and transmitted to turn the United States’ lights back on? Moreover, how might such a catastrophe occur in the first place? Perhaps the more ominous question is not how, but whether or not we can survive such circumstances if they persist in the long term.

The United States electric grid (‘the grid’) is the ‘largest interconnected machine’ in the world.5 It consists of more than 7000 power plants, 55,000 substations, 160,000 miles of high-voltage transmission lines and millions of low-voltage distribution lines.6 The scale and complexity of the grid in the context of the modern digital world are beyond comprehension because within it are innumerable industrial control systems; incalculable connections to digital networks; millions, if not billions, of analogue or digital sensors; many thousands of human actors; and trillions of lines of programming code.7 Further complexifying the grid is that it is comprised of generations of technologies, stitched together in ways that are not inherently secure in a world of cyber threats.8 The vastness of the grid makes security of it challenging. Likewise, the vastness of the grid makes the opportunities for intrusion seemingly infinite.

By any measure, grid failure will unleash a parade of horrors. Stores would close, food scarcity would follow, communication would cease, garbage would pile up, planes would be grounded, clean water would become a luxury, service stations would yield no fuel, hospitals would eventually go dark, financial transactions would stop, and this is only the tip of the iceberg – in a prolonged grid failure social chaos would reign, once-eradicated diseases would re-emerge and, increasingly, hope of returning to a normal life would fade.9 The notion of complete grid failure, once relegated to science fiction comics or James Bond movies, is now not only possible but also one of the most pressing national security threats today.10

### Impact---CI---AT: No Spillover---2AC

#### It's interdependent---individual failures cascade.

Manheim ’20 [David; September 1; Lead Researcher at 1Day Sooner Inc., Former Contract Researcher at the Future of Humanity Institute at Oxford University; Futures, “The Fragile World Hypothesis: Complexity, Fragility, and Systemic Existential Risk,” vol. 122]

3. Fragility and Systemic Risk

As technologies develop, they often build on one another, so that the continued operation of the system depends on a growing set of other systems. The way that failure occurs and propagates in such systems is non-obvious, but it is largely dependent on the topology of the interdependence between components. Pastor-Satorras, Castellano, Van Mieghem, and Vespignani (2015) Simple dependencies, where a system requires the functioning of every component, can make the resulting system of systems more fragile than the components. A very basic model of this shows that given a system-of-systems with N components, each of which independently can fail at the rate Fi the failure rate is Text

Description automatically generated. While this grows more slowly than the sum of the individual failure rates as new systems are added, it is also far higher than the average failure rate of those individual systems.

As a concrete example, the peak of efficient farming once required family farms to depend on a family to manage the farm, a blacksmith to make horseshoes and plows, and draft animals to pull them. Losing any one of these would be enough to (eventually) make the system unable to continue, and there was some risk that this would occur. Still, the limited number of inputs and the substitutability of other inputs made such systems fairly stable - especially because many risks were uncorrelated across farms, and could often be addressed by borrowing from other farms nearby.

The farms of today, of course, are not nearly as simple. They require everything from satellite GPS systems to pinpoint locations, to the semiconductors and fabrication plants used to make specific integrated chips used in the farm equipment, to internet connectivity to run machine learning algorithms using collected data and satellite imagery on remote servers. Zubarev, Fomin, and Zubarev (2019) Modern agribusiness depends on everything from finding and hiring skilled laborers to manage complex machinery, to managing regulatory, financial, and other factors critical to farm operation. Kingwell (2011) These are often more tightly correlated across an economy, increasing risk. Beyond that, managing these farms requires understanding “human, technical, economic, financial, risk, institutional and social” issues, as Lewis et al. noted more than a decade ago. Lewis, Malcolm, and Steed (2006)

The risk is likely not yet critical, but it seems clear that dependence is growing, and the ability to use backup systems can be lost. For example, if remote servers become unavailable, local corn farms may lack the information needed to decide where to increase and decrease watering levels, or even lose the ability to run their computer-controlled irrigation systems. Similarly, decades ago supplies and ordering were managed on paper, and now, without the servers running Software-as-a-Service supply-chain-management software, the dairy farm down the road may not have access to an inventory of their supplies or know what amounts of products are needed or what they have historically ordered, and end up unable to feed their cows.

The inter-dependencies in such systems are more complex than the above model allows, but more complex analyses, such as those employing percolation analysis to understand mutual interdependency of multiple networks, Buldyrev, Parshani, Gerald Paul, Stanley, and Havlin (2010) show the same trend. That is, interdependent systems where failures can propagate can be far more likely to fail than the average rate at which the individual systems’ components fail. Worse, analysis of “high–value, technology– and engineering–intensive products or systems…used to produce consumer goods and services” has shown that the failure rates are nearly-additive, and worse, are hard to identify. Yeo and Ren (2009)

It should be noted that modern computer networks do not display such fragility, but this is a function of intentional design. Metcalfe and Boggs (1976) Simple network structures, such as lines or rings, are far more prone to failure Clark, Pogran, and Reed (1978). That is, unless a system was designed for resilience, resilience should not be expected. And when technological systems are made efficient and complex, they tend to be tightly coupled - meaning that failure in one place spreads Bookstaber (2007).

3.1. Inevitable Technological Fragility Hypothesis

The proposal of this paper, to provide an addendum to Bostrom's hypothesis, is that if technological development continues indefinitely, systemic fragility will increase to the point that the possibility of a shock sufficient for complete collapse approaches certainty.

This hypothesis rests on a number of assumptions, but there are also a variety of reasons to find it plausible and concerning. To lay these out clearly, we will first consider the question of how and why individual systems are fragile, then make an argument that it is at least plausible that the multiple interconnected systems and systems-of-systems which are necessary for much of modern civilization not only fail to address this risk, but multiply it.

4. Single-System Complexity and Fragility

The key question so far is whether fragility increases over time as systems are built. The answer to that question depends on a combination of factors that can push in either direction. These include increasing complexity of systems, the economic incentives for efficiency over robustness and the resulting levels of investment in resilience, the failure rates of individual components and systems, as well as the way in which systems-of-systems (and systems-of-systems-of-systems) are interrelated, and the extent to which systems and their interdependencies are designed to be robust.

Even the claim of inevitable fragility in individual systems makes several assumptions about how fragility increases. Before looking at the systemic question of how fragility could lead to collapse, we will outline these assumptions. Note that these are in fact assumptions, rather than claims - if any one of them is false in ways that are outlined, it would refute the hypothesis. The third assumption is particularly critical, and will be explored further in the next subsection.

First, for fragility to matter, the current trend of efficiency-increasing and resilience-decreasing technologies must continue to apply to at least one critical system, such as agriculture, communication, or transport. If this is wrong, and future white-ball / safe exploration technologies are ones that favor robustness over efficiency in all such critical domains, the trend would reverse. For instance, distributed fault tolerant computing arguably increases both efficiency and robustness. Most new technologies move in the opposite direction, but if enough resilience increasing technology is found, the balance could shift.

Second, the argument for increasing fragility assumes that economic growth continues to absorb human effort in a way that does not lead to overabundant resources. In Eric Drexler's ’Paretotopia‘ scenario, increased resources are unmatched by increased demand. Drexler (2019) In that future case, resources are abundant enough that robustness is easy to achieve. This second scenario also assumes the absence of supercharged competition that uses the newly abundant resources. This would not occur, for example, in Hanson's proposed default “Em” scenario, where human-based intelligences are simulated computationally, leading to a reduction rather than an increase in surplus that could be redirected to robustness for lack of other needs. Hanson (2016)

Third, it assumes that fragility is relatively hard to identify, such that at least some failures will be unanticipated. This has been true historically, but it is possible that future developments would reverse this trend, making the search for increased robustness itself efficient enough to counterbalance the more general and destabilizing increased fragility that new technology allows. If failures do become easy to anticipate, more expensive general resilience can be replaced with more specific redundancies targeted to the exact failure modes identified.

4.1. Non-Obvious Fragility

As mentioned, hard-to-identify fragility is a key assumption. Broadly speaking, non-obvious fragility is the result of planning for efficiency, instead of designing for redundancy, fault tolerance, or even provable safety. This is a fairly general fact about any control system. Paattilammi and Makila (2000) The concrete result of the current optimization shows clear signs of producing fragile results. One example is the proliferation of disposable technology, such as fragile smartphones designed to be replaced rather than fixed or upgraded. Failure of these optimized devices is normal, and while mitigating failure is important, it is often the case that risk must be accepted, rather than avoided. Perrow (2011) This type of fragility is obvious and anticipated, rather than non-obvious and worrying. For example, individual computers are fragile, and components fail frequently. For this reason, in high-reliability computer systems, a variety of mechanisms are in place to compensate, including redundant online systems for data storage, Chen, Lee, Gibson, Katz, and Patterson (1994) or methods to address other hardware failures. Wang, Zhang, and Xu (2017)

The fact that computer networks are not fragile, and the fragility that does exist is well understood, seems to be a counterexample. But the resilience itself is planned, in contrast to ecological systems where it is emergent - as we will discuss in detail below. This means that fault-tolerant designs are built to be tolerant of expected faults. Not only that, but resilience itself is optimized, for example, to minimize the number of backups or other costs needed to have a planned level of reliability. Rodrigues-da Silva and Crispim (2014) This creates fragility to unexpected faults, and allows the systems to operate through anticipated contingencies, but not to anything beyond that point.

4.2. Sociotechnical Resilience

Fragility of systems is not based purely on the lack of resilience of technical systems. In fact, fragility of optimized technical systems is compensated for by the greater robustness of sociological systems. The combined sociotechnical system, then, is the level at which fragility should be considered.

To reduce the fragility of sociotechnical systems, organizations can attempt to build more resilience at the organizational level. This can involve information sharing, distributed decision making, and better risk assessment. If done well, these attempts provide a sociotechnical system that compensates for technical and operation risk, but is again very different from emergent resilience. Langeland, Manheim, Mcleod, and Nacouzi (2016) Unfortunately, the interaction between humans and technology can often multiply risks, rather than mitigate them. Yeo and Ren (2009)

Another reason to think that sociotechnical resilience will not fully compensate for technological fragility is the reduced human involvement in technical systems. As automation increases, Danzig notes that humans are increasingly necessarily out-of-the-loop. Danzig (2018) He further argues that when there is competition, this dynamic is a necessary result of continued optimization.

To conclude the discussion of single-system fragility, we note that inevitable fragility of systems is not actually required for the hypothesis presented. As this section argued, it does seem plausible that in expectation, new technologies will be more fragile than those they replace. However, systemic risk can exist given the much weaker claim that specific critical systems are relied upon, and technological improvements relevant to those systems alone exhibit sufficient fragility to cause a cascading collapse. Before discussing the interaction between systems, however, it is worth considering how these human, technical, or sociotechnical systems differ from naturally resilient biological systems.

### Impact---China 5G---2AC

#### China 5G dominance causes nuclear war.

Elsa Kania 19, Adjunct Senior Fellow at the Technology and National Security Program at the Center for a New American Security, 11/7/2019, "Securing Our 5G Future," No Publication, <https://www.cnas.org/publications/reports/securing-our-5g-future>

China’s quest for 5G dominance has played out within a complex technological and geopolitical landscape.108 Indeed, different countries have their own security concerns and considerations, but not all share American assessments of the severity of these risks. Insofar as American policymakers see China as a great power rival and strategic competitor, allowing Chinese companies to play a key role in American critical infrastructure, or that of U.S. allies and partners, presents grave threats that are untenable and unacceptable for the United States, not only espionage but also outright subversion of this critical infrastructure.109 Yet Huawei has continued to expand its global presence, and the U.S. government has yet to present a viable and attractive alternative to working with Huawei. Many countries may have sunk costs and be “locked in” already to this choice based on earlier decisions, which raises concerns about not only security but also fair competition.110 However, it is encouraging to see emerging consensus among like-minded countries about potential principles and shared approaches to 5G security, particularly through the progress of a recent conference on 5G security in Prague.111

The age of 5G will present new risks and novel threats of disruption or exploitation. 5G involves far more than just new and faster wireless networks; it will be a vital component of future critical infrastructure. Consequently, the cybersecurity of 5G networks could prove uniquely challenging, considering the high levels of complexity and much greater potential for damage in the case of an attack. Not only the confidentiality of data on 5G networks but also questions of integrity and assurance will become urgent challenges. Whereas most cyberattacks to date have involved only data theft, an attack against future 5G networks could cause massive damage that might threaten public safety and critical industries in future smart cities.112 The often subpar security of IoT devices, of which there are an estimated 20 billion globally and growing, also presents serious reasons for concern. A high proportion of devices on the U.S. market have been made in China by companies with very poor track records on security.113 While vulnerabilities have been and remain a major concern in the telecom industry for 3G and 4G, the stakes will be even higher for securing 5G networks at all stages of their life cycles.114 In some cases, supply chains could be weaponized deliberately by adversaries that may prefer to “win without fighting.”115 The exclusion of high-risk vendors is an important measure to mitigate risk but does not constitute a complete solution.

5G must be designed and implemented with a holistic approach to security in mind from the start. The development of secure networks must entail more than simply excluding high-risk vendors, requiring rigorous, ongoing testing and screening. Indeed, careful scrutiny should be extended to all aspects of the production, construction, and management of these networks, involving screening of the security of all vendors and carriers. If an end-to-end approach to security is effectively implemented, 5G could prove more secure than our existing networks and critical infrastructure, but the consequences of insecurity would be far graver. In public debates on 5G security, the call and search for a “smoking gun” has been problematic. This framing of the issue has often distracted policymakers from thinking about the greater challenge of mitigating vulnerabilities that tend to be pervasive. Bugs can be just as problematic as backdoors. It is inherently challenging to differentiate an accidental vulnerability from one that is deliberately introduced. The primary difference is intent, which cannot be discerned from code alone. It is encouraging that the 3GPP’s SA3 working group is focusing on security, seeking to ensure that such security concerns will shape the development of standards.116 However, industry and government are just starting to grapple with the full range of issues in play.

Given the gravity of these security challenges, the apparent centrality of Chinese companies in the global development of 5G has raised intense concerns. There is a very real risk that vulnerabilities in networks, whether the result of poor security practices or deliberate introduction of backdoors, could be weaponized for leverage or coercive purposes, particularly in a crisis or conflict scenario. Considering China’s history of IP theft and cyberespionage, there is also a real risk such networks could be exploited for purposes of espionage.117 As a Chinese company, Huawei also would be subject to a number of legal demands, regulatory requirements, and mechanisms of coercion that are often ambiguous and expansive.118 Regardless of whether Huawei’s leadership may wish to disregard an order from the Chinese government, China lacks an independent judiciary system for company leaders to plead their case against the government, as Apple did in the United States when it fought an FBI order to unlock an iPhone. Huawei’s claims that it would “say no” to the Chinese government are not credible without indications of the company’s actual ability to do so.

Even if Huawei is given the full benefit of the doubt, despite its history and apparent involvement with the Chinese military and intelligence organizations, Huawei’s products and services have been assessed to be highly insecure, with a much greater prevalence of vulnerabilities relative to their primary competitors.119 Moreover, there are reasons to question whether knowledge of any bugs in its equipment could be shared more readily with China’s Ministry of State Security (MSS). This risk may be heightened given the influence of MSS in China’s vulnerabilities database, not to mention Huawei’s historical and continued linkages to the Chinese People’s Liberation Army, including military intelligence.120 For the United States, these risks and security concerns are inextricable from today’s geopolitical exigencies, insofar as the U.S.-China rivalry encompasses scenarios for which there is a nonzero probability of conflict, including over Taiwan. Consistently, Chinese military writings have highlighted the potential for cyberattacks on critical infrastructure as a prelude to outright warfare.121 The presence of equipment from high-risk vendors, such as Huawei, even in rural telecoms is concerning, considering that some of these networks are near military bases, which raises risks of espionage or exploitation.

5G security presents a global challenge that will demand creative and cooperative solutions. Huawei will likely remain a major player in 5G in a number of countries, including some U.S. allies and partners, that believe the benefits of partnering with it outweigh the risks. Although a criteria-based calculation of risk provides compelling arguments for exclusion of such highly risky players, many nations could still continue current collaborations with Huawei in ways that exacerbate global risks to this emergent ecosystem. Even if the United States were to succeed in fully securing its own 5G networks, U.S. data and entities may remain reliant, including for military and commercial activities, upon overseas digital infrastructure that could prove highly vulnerable.The presence of Huawei’s equipment in the critical infrastructure of U.S. allies and partners, whose support or location as a staging ground the U.S. military might require to fulfill its treaty obligations in the event of a crisis or conflict, also creates new risks, to an extent that could undermine U.S. capabilities for command and control and power projection. As Dan Coats, had warned during his time as director of national intelligence (DNI), “U.S. data will increasingly flow across foreign-produced equipment and foreign-controlled networks, raising the risk of foreign access and denial of service.” 122

### Impact---Democracy---2AC

#### China 5G enables digital authoritarianism and collapses democracy.

Rumana Ahmed 21, consultant on democracy and technology for the National Democratic Institute and a Truman National Security Fellow; and Moira Whelan, the director of democracy and technology at the National Democratic Institute, 7/17/2021, "China Knows the Power of 5G. Why Doesn’t the U.S.?," Foreign Policy, https://foreignpolicy.com/2021/07/17/china-5g-us-g7-b3w-technology-infrastructure/, RMax

Biden’s plan is an important step to combating China’s rising influence. But it needs to prioritize technology more, especially 5G, which is carrying the world into the next era of the internet. The B3W plan doesn’t explicitly mention 5G, even though that technology is beginning to transform how we communicate and live by expanding information access, automating everyday services, and advancing smart cities and policing. Essentially, 5G has the power to affect all four areas of the B3W plan, and how it is built, used, and governed can tip the scales in favor of authoritarianism or democracy in any given country. The G-7 should recognize 5G’s power—and the risks it poses in the wrong hands—by making 5G a central thread that ties its infrastructure plan together and promoting it in B3W.

In recent years, the U.S. security community has woken up to the threats of the Chinese Communist Party’s technology agenda. The party’s approach centers on two tactics: a series of laws that require Chinese companies, including those providing services abroad, to give Beijing unfettered access to data and the global export of 5G hardware. Chinese business leaders go to other countries bearing inexpensive hardware and the promise of economic advancement, all for the price of control over data that can be accessed by Beijing or local authoritarian regimes.

5G is an easy tool to weaponize. As demand for it grows worldwide, citizens and infrastructure are becoming increasingly reliant on it. As of February, 131 countries announced plans to invest in 5G, which will be foundational for future internet technologies. Like the internet and social media, 5G promises greater access to information. But it also allows more data to be gathered than ever before, and any 5G-backed technology can expedite and expand the scope and scale of what people—and governments—can do with that information.

5G adoption in a country inclined toward authoritarianism makes autocrats more efficient. In those countries, decision-making around 5G adoption occurs almost exclusively in executive branches of government with little to no oversight, giving leaders broad control over data flow and governance. As a result, mass surveillance can ensue, as well as large-scale human rights abuses through automated discrimination, censorship, and persecution—much like what is taking place against Uyghurs in China’s Xinjiang region. Leaders with access to 5G-backed artificial intelligence capabilities and real-time citizen information are able to employ subversive disinformation campaigns with greater reach to fuel violent polarization. Meanwhile, internet shutdowns only increase in frequency and target political opponents, dissidents, and journalists, which has already happened in Myanmar, Kashmir, Chad, and Nigeria.

Already, the export of Chinese technologies and tools to Latin America, Africa, and Southeast Asia has coincided with a rise of digital authoritarianism. It has given dictators, including Venezuela’s Nicolás Maduro and Uganda’s Yoweri Museveni, broader control over everything from data flow to airwaves. Parliament buildings have been wired, political opponents threatened, and citizens surveilled and censored using technologies produced and serviced by Chinese companies, such as Huawei and ZTE.

But that doesn’t mean 5G is inherently dangerous. Democracies have every reason to pursue the technological promise of 5G, as increased data capacity can make states more efficient and help governments deliver on services. Public utilities, for instance, could be made greener through automated regulation with 5G technology. Perhaps the greatest promise of 5G, though, is that it enables more people to access digital technologies. By delivering 5G to marginalized communities, which face a growing digital divide that especially affects women and rural areas, countries can increase opportunity for greater information flow, access to education tools, and other societal benefits.

In healthy democracies, the oversight of these technologies should respect human rights and privacy and shouldn’t be conducted behind closed doors. Companies, civil society actors, and the general public should work with the government to create rules around data in a transparent way. The good news is that Biden’s B3W plan makes clear that he understands the importance of technology in shaping the norms of the international system to embrace human rights and putting decision-making in the hands of many stakeholders. But the clock is ticking.

Right now, China offers cheap technology to telecommunications providers in countries with few regulations around transparency and multi-stakeholder engagement. G-7 countries can’t simply subsidize rights-respecting companies and expect them to be competitive in those markets. Instead, they must work together across regions to implement global standards and practices around the security of 5G equipment and 5G ecosystems and the flow and control of data, especially as it pertains to data privacy, internet freedom, and human rights. They also need to increase investments into future-generation technologies and incentivize 5G development in marginalized communities worldwide to address current digital, social, and economic inequality. If they act too slowly, they’ll cede the digital landscape to Beijing and its authoritarian friends. It is a tremendous challenge, but the G-7 democracies are poised for great success if they work together.

For now, though, an effective global plan to influence conversations around technology and democracy—and 5G’s role in them—remains absent. For instance, clear international consequences for digital rights violations are nonexistent. One promising framework for the United States’ approach to technology leadership and global cooperation was laid out at the Global Emerging Technology Summit this week by U.S. National Security Advisor Jake Sullivan and Secretary of State Antony Blinken. In the fall, the United Kingdom will host the Future Tech Forum, the Danish government will hold a technology conference, and the Czech government will convene a 5G conference. These events will be invaluable in the fight to drive the world toward a cooperative, values-based approach to technology governance. As the international community continues to take these issues seriously, the United States and regional leaders worldwide will need to set global standards and ensure that the technology infrastructure market has more diverse vendors, affordable equipment options, and research and development investments that create secure technologies. Governments must work with private companies, think tanks, and civil society to ensure that these changes are more than a pipe dream.

Technology is inseparable from the future of democracy, and Biden’s B3W effort is the first step in the long road to developing these global technology standards that prioritize and protect data privacy, open digital spaces, and human rights. What Biden needs to acknowledge is that technologies and infrastructures reliant on insecure 5G networks in particular have great potential to harm democracy. A central question for our time is how successful democracies can be maintained and strengthened as the internet pervades more and more of citizens’ daily lives. Focusing on 5G will have the most immediate impact—and curtail the worst results.

### Impact---Heg---2AC

#### The 5G race determines global influence---US victory ensures national security is preserved.

Graham Lampa 19, former National Security Advisor to the President, retired Marine Corps four-star general, 9/9/2019, "Recommendations on 5G and national security," <https://www.atlanticcouncil.org/content-series/strategic-insights-memos/recommendations-on-5g-and-national-security/>, RMax

The 5G Technology Race

The nation that leads in developing and widely deploying 5G technology will have an important first-mover advantage, with both economic and national security implications. Chinese national champion Huawei is the current global leader in 5G, and China’s ZTE is also a major player in the industry. Huawei is aggressively pursuing export of its 5G systems to install digital infrastructure around the globe. Huawei is an attractive option to many nations because it is cheaper than its competitors. The products of firms competing with Chinese companies will be more expensive because of unfair subsidies from the Chinese Communist Party, which artificially reduce prices.

Huawei is a tool of state power and a critical asset in China’s global economic and geopolitical competitions and ambitions. Huawei faces competition from Samsung USA and others as an end-to-end producer, and still other companies produce 5G components (such as antennae, chips, and base station architecture) including Ericsson, Nokia, and Qualcomm. These firms are more expensive because they are not the beneficiaries of unfair state subsidies. However, they offer other advantages, including enhanced security, more rigorous training of personnel, protection of intellectual property, and privacy. From a national security perspective, this race is not about US commercial market share, but rather mitigating China’s ability to influence US allies and security partners.

Why is 5G Important for National Security?

If China controls the digital infrastructure of the 21st century, it will exploit this position for its national security purposes and be capable of coercive leverage over the United States and allies. These networks will process all manner of data, and China certainly will use the network to conduct espionage on the United States and allies for national security and industrial purposes. It will allow for the emplacement of “backdoors” in networks that could be activated to conduct catastrophic cyberattacks on US and allied “smart cities” in the event of conflict. Put another way, Huawei’s 5G technology is the 21stcentury version of the mythological Trojan Horse. The spread of Chinese 5G networks will threaten NATO and allied interoperability, as the United States will become unable and unwilling to integrate its secure 5G network with any aspect of Chinese systems.

Finally, this race, and its outcome, rises to the level of importance of such projects as the Manhattan Project and the ‘man on the moon’ efforts of the 20th century. 21st-century security, both public and private, will be profoundly affected by the decisions taken in the next few months.

For countries who select the Chinese alternative and the consequences attendant to such a decision, the costs of reversal will increase exponentially as they proceed. For these reasons, the United States and several close allies (the United Kingdom, Australia, New Zealand, Japan, Canada, Poland, France, and others) have either banned or are considering bans on Huawei 5G systems. However, many other states, including US allies, have installed or are considering installing Huawei’s networks.

This is an urgent problem that will shape economies and societies for future generations. The infrastructure investment decisions that will determine the future 5G architecture will be made in the coming weeks and months, not years.

### Impact---Smart Cities---2AC

#### Unsustainable urbanization causes extinction---smart cities are key.

Cribb ’17 [Julian; author, journalist, editor and science communicator. He is principal of Julian Cribb & Associates who provide specialist consultancy in the communication of science, agriculture, food, mining, energy and the environment. His career includes appointments as newspaper editor, scientific editor for The Pic credit: J. Carl Ganter Australian newspaper, director of national awareness for Australia’s science agency CSIRO, member of numerous scientific boards and advisory panels, and president of national professional bodies for agricultural journalism and science communication. His published work includes over 8000 articles, 3000 media releases and eight books. He has received 32 awards for journalism. His internationally-acclaimed book, The Coming Famine explores the question of whether we can feed humanity through the mid-century peak in numbers and food demand. <KEN> “The Urbanite (Homo Urbanus).” Surviving the 21st Century. Springer. doi:10.1007/978-3-319-41270-2\_8.]

By the mid-twenty-first century the world’s cities will be home to approaching eight billion inhabitants and will carpet an area of the planet’s surface the size of China. Several megacities will have 20, 30, and even 40 million people. The largest city on Earth will be Guangzhou-Shenzen, which already has an estimated 120 million citizens crowded into in its greater metropolitan area (Vidal 2010 ).

By the 2050s these colossal conurbations will absorb 4.5 trillion tonnes of fresh water for domestic, urban and industrial purposes, and consume around 75 billion tonnes of metals, materials and resources every year. Their very existence will depend on the preservation of a precarious balance between the essential resources they need for survival and growth—and the capacity of the Earth to supply them. Furthermore, they will generate equally phenomenal volumes of waste, reaching an alpine 2.2 billion tonnes by 2025 ( World Bank )—an average of six million tonnes a day—and probably doubling again by the 2050s, in line with economic demand for material goods and food. In the words of the Global Footprint Network “The global effort for sustainability will be won, or lost, in the world’s cities” (Global Footprint Network 2015).

As we have seen in the case of food (Chap. 7), these giant cities exist on a razor’s edge, at risk of resource crises for which none of them are fully- prepared. They are potential targets for weapons of mass destruction (Chap. 4). They are humicribs for emerging pandemic diseases, breeding grounds for crime and hatcheries for unregulated advances in biotechnology, nanoscience, chemistry and artificial intelligence.

### Impact---AT: Smart Cities Bad---2AC

#### Smart cities inevitable.

Robert Muggah 21, principal at the SecDev Group and co-founder of the Igarape Institute; and Greg Walton, fellow at the SecDev Group and a researcher at the Oxford Internet Institute, 4/17/2021, "‘Smart’ Cities Are Surveilled Cities," Foreign Policy, <https://foreignpolicy.com/2021/04/17/smart-cities-surveillance-privacy-digital-threats-internet-of-things-5g/>, RMax

Cities around the world are getting smarter. A growing number even designated themselves “smart cities.” There are, of course, as many definitions of smart cities as there are cities professing to be smart. Very generally, smart cities deploy a host of information communication technologies—including high-speed communication networks, sensors, and mobile phone apps—to boost mobility and connectivity, supercharge the digital economy, increase energy efficiency, improve the delivery of services, and generally raise the level of their residents’ welfare. Becoming “smart” typically involves harnessing troves of data to optimize city functions—from more efficient use of utilities and other services to reducing traffic congestion and pollution—all with a view to empowering public authorities and residents.

However one defines them, data-enabled cities are booming. By one estimate, there are over a thousand smart city projects underway around the world. Rankings and indices are also proliferating, with such cities as Singapore, Helsinki, Seoul, and Zurich routinely topping the list. Notwithstanding global enthusiasm for hyperconnected cities, this futuristic wired urban world has a dark side. What’s more, the pitfalls may soon outweigh the supposed benefits.

## AT: 5G Bad

### 5G Bad---2AC

#### 5G is safer than current technology---other devices emit more power.

Paul Lee et al 20 (Paul Lee is a UK Partner and the Global Head of Research for the technology, media, and telecommunications (TMT) industry at Deloitte. 12-7-2020, "5g health risks debunked," Deloitte Insights, <https://www2.deloitte.com/us/en/insights/industry/technology/technology-media-and-telecom-predictions/2021/5g-radiation-dangers-health-concerns.html>) //billy

Extremely low power, extremely low risk

Of course, nonionizing radiation is not always completely harmless. The most common form of nonionizing radiation is visible light, which has a higher energy level than radio waves. An excess of visible light—or even radio waves—can produce heat, and in extreme cases cause burns and body tissue damage. However, the power behind the radiofrequency radiation generated by mobile networks is controlled and poses virtually no risk to consumers.

Power transmission from mobile telephony, including 5G, is far lower than that from light bulbs, TV, radio towers, or even sunlight on an overcast day. The quantity of this power is measured in watts, and a single watt is a tiny quantity of energy. The power transmitted by the mobile phones used in 2021 and into the foreseeable future can reach up to two watts, depending on the age of the phone; it can be as low as 0.001 watt, with the vast majority of devices in use this year peaking at 1 watt. By comparison, the power transmitted by CB radios, which have been in use for decades, reaches up to four watts.8

As with a car journey, the shorter the distance, the less the power required. A phone held next to the head or kept in a pocket would have the greatest impact. The radiation level from a phone or speaker placed on a table near the user would be lower. A smartphone will transmit more power when base stations are relatively distant, but most smartphones are used predominantly indoors, and tend to be connected to Wi-Fi routers (which are effectively miniature base stations), which are often mere meters away. In all of these cases, the amount of power transmitted is minimal—certainly much lower than required to be harmful. Further, a smartphone transmits power only when sending or receiving data, a mechanism designed to prolong battery life.

The power generated by mobile network base stations is similarly low. A base station’s transmissions range in power from a quarter of a watt for a small cell (which would often be indoors and cover a small range) to 200 watts9 for a minority of 5G base stations.10 More typically, an outdoor base station with the greatest range would have a power output of between 10 and 100 watts. The output of indoor base stations, which usually have a range of hundreds of meters or less, is much lower.11

As with a phone, a base station’s power level declines with distance from its transmitter. An individual 100 meters away from a 5G macrocell antenna located at 30 meters’ height would absorb less than one microwatt (one-thousandth of a watt) of power.12 When one is directly next to a base station supporting any generation of mobile standard (not just 5G), exposure limits may be exceeded.13 But these areas are inaccessible to the public, sometimes because of their height (20 meters or higher for larger sites), their location (often at the top of buildings), or their design (because the units are enclosed). In the case of indoor base stations, excessive exposure would only happen within a few centimeters of the transmitter.

Average broadcast transmission power has declined as the number of base stations deployed has increased, resulting in a smaller distance between base stations and users. Transmitter power levels for 1G and 2G networks were far more powerful, on average, than those used for 4G or 5G, since 1G and 2G transmitters covered a far greater range, often tens of kilometers in each direction. In contrast, 4G and 5G masts in city centers and other traditionally congested areas may cover just 100 meters.

It is worth reiterating how minuscule a watt is. An incandescent bulb, which radiates light via a wire filament that is heated until it glows, is rated between 25 to 200 watts. In domestic settings, people may be less than half a meter away from a light bulb. A person this distance from a 25-watt bulb would be exposed to thousands of times more radiation than an individual who was 10 meters (unusually close) to a relatively high-powered 5G base station.14 This is not just the case in 2021—it should hold true always. Similarly, people absorb five times more radio frequency exposure from FM radio and television broadcasts than from mobile network base stations.15 The broadcaster transmitter power levels used for TV and FM radio can reach up to 100,000 watts.16 For AM radio, the transmission power may reach 500,000 watts.17

Humans have coexisted with incandescent light bulbs, and their radiation, since the 1880s with no known malign effects (except, of course, from being burnt from touching a lit bulb). As for broadcast power, the first television station went on the air in 1928,18 and the first commercial radio station launched in 192019—yet no reliable account of people being harmed by the radiation these stations generate has ever been reported.

5G is even safer than previous mobile network generations

In 2021, consumers who are concerned about the health impacts of mobile networks are likely to be most worried about 5G, the latest generation of mobile technology. However, in some ways, 5G is likely to have even lower potential health impacts than earlier generations of mobile telephony.

5G has been designed to use less power than previous generations to reduce operational costs; as a result, it emits less power as well. This is accomplished via the new, advanced radio and core architecture used in the 5G standard, with 5G networks assisting 5G devices in minimizing power transmit levels.20 5G base stations also can be put into sleep mode when there are no active users (for example, at night). This capability is not available with 4G networks, which transmit control signals even when there are no users in range.21

5G also incorporates a technique known as beamforming, an approach that involves directing a narrow beam of radio waves to the user device (such as a smartphone). This method is equivalent to directing a narrow beam of light from a pocket flashlight at a target, focusing the radio waves on the device. This method not only enables higher connection speeds, but also leads to lower radio wave exposure than prior network generations, which would often spread radio waves across a wide arc, similar to a car’s headlight.

Some people may conflate the risks associated with beamforming with industrial-grade laser beams. A manufacturing-grade laser beam, which is 100 million times as powerful as a typical laser pointer, is capable of melting steel.23 But beamforming in 5G networks involves innocuous levels of power.

As a final note, tests of 5G sites in 2020 by regulators such as Ofcom in the United Kingdom have found that their EMF levels are well within International Commission on Non-Ionizing Radiation Protection (ICNIRP) guidelines.24 ICNIRP is an independent scientific commission based in Germany that works with the World Health Organization (WHO), the International Labour Organization (ILO), and the European Commission. The highest EMF level recorded among the 22 locations tested was 1.5% of the acceptable level—in other words, 98.5% below the acceptable level. Most of the sites tested supported four generations of mobile technology; that is, a combination of 2G, 3G, 4G, and 5G (in many markets, 5G-only base stations remain relatively rare). At all of these sites, 5G contributed the least to the EMF fields measured. In 19 of the 22 locations, the highest 5G band value was less than 0.01% of the acceptable ICNIRP level.

### 5G Bad---AT: Bees---2AC

#### 5G doesn't harm bees - their studies are based on incomplete data

McAfee 19 [Alison McAfee is a honey bee scientist and a science writer; "Why We Shouldn’t Fear 5G"; 10-1-2019; American Bee Journal; https://americanbeejournal.com/why-we-shouldnt-fear-5g/]//AShah

Adoption of 5G cell phone networks will lead to more cell towers, but there’s no good reason to expect it to harm honey bees

The next generation of cell phone connectivity — the 5G network — has been launched. Most countries are projected to adopt the technology by 2020, and we should expect download speeds ten to twenty times faster than 4G as well as higher network capacity (i.e., more devices can be used on a network simultaneously), feeding our existing data addictions. For some people, the 5G launch has also renewed old concerns that cell phone-generated electromagnetic waves could be interfering with honey bee navigation.

It all started in 2006, when Dr. Jochen Kuhn, a professor at Landau University, Germany, and his colleagues released the seminal study (which, to the best of my knowledge, was never peer reviewed).1 The researchers placed DECT docking stations — digital enhanced cordless telecommunications stations, the kind used for cordless landline telephones — inside two mini-hives and powered them up. The two other hives did not get docking stations. They then trapped 25 bees at the entrance of each hive, released them 800 meters away, and recorded how many made their way home. They also measured comb areas in the hives, after giving the mini-colonies a chance to build up. The bees from docking-station-hives, as the old story goes, built less comb and were worse at finding their way home. The next generation of cell phone connectivity — the 5G network — has been launched. Most countries are projected to adopt the technology by 2020, and we should expect download speeds ten to twenty times faster than 4G as well as higher network capacity (i.e., more devices can be used on a network simultaneously), feeding our existing data addictions. For some people, the 5G launch has also renewed old concerns that cell phone-generated electromagnetic waves could be interfering with honey bee navigation.

Data from two hives is obviously not enough to make any solid conclusions, no matter how well an experiment is designed. And well-designed, this wasn’t. The authors recognized this, writing that “because of the explorative character of [the] study we refrain from a differentiated statistical analysis.” In other words, the data were too sparse to apply standard statistical tests that all credible scientists use. And it didn’t even involve cell phones.

### 5G Bad---Enegy---2AC

**The transition period between 4G and 5G is not detrimental—overall, long term use of 5G increases energy efficiency**

Kelly **Hill, 2022;** executive editor at RCR Wireless News, M.A. from UC Berkley in Journalism; “Parsing the 5G Power Equation: Is 5G Actually Greener? https://www.rcrwireless.com/20220124/5g/parsing-the-5g-power-equation-is-5g-actually-greener

In comparison, 5G offers a far more **efficient** overall structure in terms of its physical layer and need for such reference signals, according to Dr. Nishith Tripathi, a wireless researcher and adjunct associate professor of electrical and computer engineering at Virginia Tech (formerly of Samsung Research America). “We have taken care to make this a physical layer operation that is very efficient, so it will **consume less power** to get the information that we want,” he explains. “But it takes time for technology to stabilize, and [move] away from NonStandalone, so we **can reap the benefits of that 5G capability.”**

Fundamentally, 5G provides “much better **support for implementing energy-saving features** in network products,” according to an Ericsson blog post from October 2021. “The crucial difference is the vastly improved support for **energy savings** during low-to-medium traffic.”

Power-saving mechanisms also offer the possibility that instead of steady-state power consumption, that at times of low usage, radio channels could be shut down, explains Tripathi.

In LTE, the number and timing of synchronization and reference signals provide very little space for time gaps, where “micro-sleep” energy-saving features can operate**. 5G can allow gaps in transmission** as long as 20 ms in SA and 160 ms in NSA mode, which are 100 to 800 times longer than what is allowed in LTE, along with **requiring far less “always-on” signaling,** according to Ericsson. “Since more components can be put in sleep mode for longer periods, there is a significant potential to **reduce energy consumption of 5G-NR products** and eventually the overall network energy consumption,” Ericsson’s experts write. However, they also point out that the network should be built with precision in order to take advantage of power-saving features – so that high-capacity products are only put where that capacity is needed.

In current 5G networks, the **industry may be seeing a particularly strong strain on power use** – but that may change as the tech matures. Early 5G implementations are limited in coverage, which can drain device batteries faster as the device jumps back and forth between LTE and 5G New Radio. In addition, 5G NonStandalone, the mode in which most 5G networks operate today, still relies on LTE for control-plane communications and adds more processing (and power) demand as a result. As 5G SA becomes a larger part of the network, the numbers (on a watt/bit basis) improve.

France’s telecom regulator, Arcep, recently published its analysis of energy assessment of 4G versus 5G, in the context of how each technology would perform under traffic growth assumptions through 2028 in the 3.5 GHz band. What it found was that **initially, 5G generated an increas**e in energy consumption – just how long that period was, depended on the specific 5G rollout scenario being modeled. But generally, the study concluded, “**energy efficiency gains achieved from 5G deployment** will begin in 2023 and be clear by 2028 in the most densely populated areas.”

**Compared to 4G-only densification** strategy over the same time period, Arcep said, 5G deployment enabled total energy savings of up to ten times 2020 consumption levels by 2028, and was associated with a corresponding decrease of greenhouse gas (GHG) emissions of up to eight times 2020 GHG emissions. However, the regulator added, “In less densely populated areas, however, where traffic density is lower, virtually non-existent gains will not be seen until 2025 at the earliest, and by 2028 at the latest.”

So essentially, another “yes, but …” Yes, 5G will consume a great deal of energy—but 4G would consume even more under the same conditions. **Progress in energy savings, as in many things, is incremental.**

“I believe that as time progresses, we will become more and more green in terms of the ‘G’,” said Tripathi. “So 5G, greener than 4G; and 6G will be greener than 5G. … We are working on all those things to make things a little bit greener compared to the previous generations. “Once the idea is introduced in the standard, it takes some time before they are implemented in real products,” he notes. “So things take time. But gradually, we are moving in that direction.”

### 5G Bad---AT: Environment---2AC

#### 5G is good for the environment.

Cho ’20 (Renee Cho, staff writer for the Columbia Climate School, received the Executive Education Certificate in Conservation and Sustainability from the Earth Institute Center for Environmental Sustainability, has been published by [www.insideclimatenews.com](http://www.insideclimatenews.com) and other environmental magazines, former Communications Coordinator for Riverkeeper. “The Coming 5G Revolution: How Will It Affect the Environment?” 08/13/20 <https://news.climate.columbia.edu/2020/08/13/coming-5g-revolution-will-affect-environment/#:~:text=By%20enabling%20more%20people%20to,reducing%20traffic%20congestion%20and%20idling>.) ☺

How can 5G help the environment?

The speed, capacity and connectivity of 5G will provide many opportunities to protect and preserve the environment. 5G technology with IoT will be able to increase energy efficiency, reduce greenhouse gas emissions and enable more use of renewable energy. It can help reduce air and water pollution, minimize water and food waste, and protect wildlife. It can also expand our understanding of and hence improve decision-making about weather, agriculture, pests, industry, waste reduction and much more.

According to the UN, 68 percent of the world’s population will live in cities by 2050. City governments and businesses are looking to 5G, [artificial intelligence (AI)](https://blogs.ei.columbia.edu/2018/06/05/artificial-intelligence-climate-environment/)and IoT technology to create smart cities where sensors, cameras and smart phones will be linked; the connectivity and speed of these networks will enable cities to be better managed and more efficient and sustainable.

Here are just some of the ways, 5G can benefit the environment.

Reducing energy consumption and emissions

International standards have called for 5G to require much less energy to run than 4G, which means using less power while transmitting more data. For example, one kilowatt-hour (kWh) of electricity is needed to download 300 high-definition movies in 4G; with 5G, one kWh can download 5,000 ultra-high-definition movies.

5G linked with IoT will also cut energy use, because devices will be able to power up and shut down automatically when not needed. Sensors in appliances, transportation networks, buildings, factories, street lights, residences and more will monitor and analyze their energy needs and consumption in real time and automatically optimize energy use. For example, smart electricity meters installed in the Empire State Building have helped cut energy costs by 38 percent. GE’s Digital Power Plant for Steam in France, equipped with 10,000 sensors to improve plant efficiency, got the Guinness World Record for the world’s most efficient power plant.

Because saving energy also means cutting greenhouse gas emissions, GE’s Digital Power Plant software is expected to reduce carbon emissions by 3 percent and fuel use by 67,000 tons of coal per year. A study done by Ericcson, a leading information and communication technology provider, projects that IoT could cut carbon emissions 15 percent by 2030.

5G and the IoT will enable microgrids to be brought on line when the main grid fails or is unavailable. This will make it possible to better integrate intermittent renewable energy sources such as wind and solar into the grid. Ameresco, a Massachusetts-based company, replaced an old steam plant with a fully automated plant supported by 20,000 solar modules and its own microgrid at the U.S. Marine Corps Recruit Depot on Parris Island, S.C. The system reduced energy use by 75 percent.

By enabling more people to work or access entertainment remotely and avoid commuting and flying for business, 5G will save energy and reduce greenhouse gas emissions from vehicles and airplanes.

If driving is a necessity, 5G can save time, fuel and vehicle emissions by reducing traffic congestion and idling. With sensors and cameras, 5G uses real time data to keep traffic flowing, changing traffic lights to avoid delay. Carnegie Mellon’s Metro21: Smart Cities Institute’s smart traffic control system, which employs radar and cameras to reduce idling, has resulted in 20 percent fewer greenhouse gas emissions in Pittsburgh. 5G can also reduce the number of cars on the road by helping drivers find parking spaces and enabling ride sharing.

Reducing water and food waste

According to the EPA, U.S. households waste one trillion gallons each year due to leaks. Smart water sensors can detect leaks, as well as water pollution and contamination.

Sensors can also optimize agricultural water use. Arable, an innovative agricultural company, uses smart agricultural sensors that incorporate weather information and soil and crop conditions to better manage irrigation and make it more efficient. The systems also monitor plant stress, nutrients and pests to help plan harvests.

The UN has estimated that about one-third of the food produced globally is wasted, which also wastes the energy and water that went into it. Agricultural sensors can detect when a plant is wilting, so they can help ensure that crops are harvested at the right time. Other sensors can detect food freshness and spoilage, so that consumers know when food is safe to eat without depending on expiration dates. 5G could eventually be used to tag all food where it’s produced, track harvest dates or identify specific animals, and then trace the smart tags as food is transported to the factory. Other sensor systems could monitor conditions in the factory, assessing the food for quality and compliance with regulations. An automated and transparent system could make sure that the correct ingredients are delivered at the right time and packaged properly. This would help reduce food waste, maximize food safety, evaluate a food’s sustainability, and allow a supply chain to respond more quickly to supply and demand issues.

Protecting nature

To keep sewage from polluting the St. Joseph River in South Bend, Ind., smart sewer technology was installed in manholes. The technology reduced sewage overflows by 70 percent —over one billion gallons a year—and saved the city more than $500 million.

Toxic blue-green algae bloom when water temperatures are warmer than usual. Nokia used 5G drones with cameras and sensors over the Baltic Sea to detect blue-green algae growth in real time. While algae are normally monitored by observation from shore, the drones made it possible to detect algae blooms in more remote areas. Getting timely information enables experts to rapidly take actions to prevent such environmental hazards.

Australian start-up Myriota and the Australian Institute of Marine Science (AIMS) are using marine buoys with satellite-connected IoT sensors to track ocean currents, sea surface water temperatures, and the barometric pressure of the ocean in real time. This helps researchers better monitor changing conditions in the ocean and understand how the ocean behaves.

Rainforest Connection, a nonprofit fighting illegal deforestation, is working with 5G and AI to protect the rainforest in Costa Rica. AI recorders recognize the sounds of chainsaws and other machinery, so they can alert rangers about illegal logging in real time. They can also distinguish the sounds of animals under stress so that rangers can respond quickly to illegal poaching.

The International Union for Conservation of Nature uses 5G geolocation technology to track the location and movements of endangered animals. And at the Chengdu Research Base of Giant Panda Breeding in China, 5G is being used to monitor panda conditions and encourage breeding. Pandas only ovulate once a year and are fertile for only 24 to 36 hours so breeding them is challenging. The technology identifies panda mating calls and plays them back to the pandas to encourage them to mate with each other.

**5G is crucial to efficient environmental sustainability in cities**

**Accenture, 2022**;Accenture plc is an Irish-American, professional services company based in Dublin, specializing in information technology services and consulting; “5G Enabled Technologies Could Solve for One-Fifth of U.S. Climate Change Target by 2025, New Study Finds” https://newsroom.accenture.com/news/5g-enabled-technologies-could-solve-for-one-fifth-of-us-climate-change-target-by-2025-new-study-finds.htm#:~:text=The%20report%2C%20titled%205G%20Connectivity,of%20additional%20abatement%20by%202025.

The report examined 31 use cases for 5G across five industry verticals: transportation and cities, manufacturing, buildings and energy, agriculture, and working, living and health. The report discusses the following three verticals in depth, where **5G will have significant downstream carbon abatement potential**:

**Transportation and cities**: 5G-enabled use cases in the ground transportation and cities vertical can total up to 86.5 MMtCO2e of carbon abatement in the U.S., thanks to reduced traffic congestion, **reduced vehicle idling** at signals and while parking, shorter routes optimization, and greater adoption and opt-ins of more **sustainable choices** such as public transportation. The carbon abatement in this vertical is **equivalent to** the carbon sequestered by **106 million acres of U.S forests** in a year.

**Manufacturing**: **5G-enabled use** cases in the manufacturing vertical can total up to 67.4 MMtCO2e of carbon abatement in the U.S., thanks to **enhanced inventory management**, real-time asset monitoring, predictive maintenance, process augmentation, and travel avoidance. The carbon abatement from inventory management by 2025 alone is equivalent to removing CO2 emissions from 17 coal fired power-plants in a year.

Energy and buildings: 5G-enabled use cases in the energy and buildings vertical can total up to 67.9 MMtCO2e of carbon abatement in the U.S., thanks to real-time monitoring, **increased green energy use**, fuel savings through reduced transport facilitated by remote operations, **building energy management systems**, commercial HVAC controls, smart meters and smart grids, and **renewable microgrids**. The carbon abatement from energy and buildings by 2025 is equivalent to removing CO2 emissions from electricity consumed by 12 million homes in a year.

“This study shows 5G networks can **bring material reductions** in our country’s carbon footprint,” said Peters Suh, Accenture’s North America Communications and Media industry lead. “The crucial piece will be how industries leverage cloud-first 5G networks to **bring greater innovation** into key operational processes. With appropriate education and ecosystem changes, organizations can reap the climate benefits of 5G across their cloud continuum, which includes everything from the public cloud to the edge."  
   
“U.S. 5G networks already cover 305 million people, we’re building out 5G faster than we built out 4G, and every day, the wireless industry is working to make these networks go faster and farther,” added Attwell Baker. “Taken together, America’s wireless ecosystem is positioning U.S. **innovators across these key industry verticals** to quickly **unlock these climate benefits.”**

### 5G Bad---AT: Disease---2AC

#### 5G doesn’t cause disease---virus can’t travel via radio waves.

Paul Lee et al 20 (Paul Lee is a UK Partner and the Global Head of Research for the technology, media, and telecommunications (TMT) industry at Deloitte. 12-7-2020, "5g health risks debunked," Deloitte Insights, <https://www2.deloitte.com/us/en/insights/industry/technology/technology-media-and-telecom-predictions/2021/5g-radiation-dangers-health-concerns.html>) //billy

5G and the spread of COVID-19

One myth about 5G’s impact on health that has been widely spread in 2020 is the fictional association between the roll-out of 5G and the spread of COVID-19.25 Put plainly, the idea that 5G transmits COVID-19 is as bogus as it is impossible. COVID-19 is a virus spread through respiratory droplets from other people. A virus does not travel via radio waves.

A variant of 5G misinformation related to COVID-19 is that 5G emits radiation that weakens people’s immune systems, making them more susceptible to illness.26 This is similarly false.

It is likely that misinformation about 5G’s relationship to COVID-19 will be as pervasive in 2021 as it was in 2020. An Ofcom survey at the end of June 2020 found that 29% of respondents had come across false or misleading information about COVID-19 in the prior week.27 The most common topic, seen by 21% of respondents, was “theories linking the origins or causes of COVID-19 to 5G technology.” Misinformation about 5G was even more prevalent earlier in the year: An Ofcom survey undertaken from April 10–12, 2020, found that 50% of respondents had seen false or misleading statements about 5G. The good news is that these people recognized the misinformation as such.28 The bad news is that the majority (57%) of those who saw what they regarded as misinformation did nothing about it.

### 5G Bad---AT: Disease---1AR

**There are no conclusive scientific studies that 5G actually harms humans—exposure levels of 5G are actually lower than the current 4G system**

Joan **Conrow, 20;** Managing editor and communications consultant at the Cornell Alliance for Science, journalist (specialty in technological misinformation); “Three reasons why 5G is unlikely to cause harm” 06/26/2020 https://allianceforscience.cornell.edu/blog/2020/06/three-reasons-why-5g-is-unlikely-to-cause-harm/

Following persistent conspiracy theories that have resulted in vandalism of 5G towers and attacks on telecom workers, a team of experts has once again considered the health and safety issues around 5G high-speed wireless communications networks.

So, what did they find? While it is obviously absurd to suggest that a biological agent like a virus can be transmitted directly over the electromagnetic spectrum, are there any actual scientifically-justified health concerns about 5G?

The new evidence-based review, which appears in Health Physics journal, concludes that there appears to be “**little or no risk of adverse health effects**” related to radiofrequency (RF) exposure from 5G systems. The paper was authored by a physician/biologist, epidemiologist, engineers and physical scientists, all working voluntarily and collaboratively on a consensus basis.

The authors explain that **5G “is not specific to frequency**” and may be deployed for operating networks currently using frequencies extending from 100s to 1,000s of MHz. It can also operate in the 10s of GHz where the wavelengths are 10 mm or less — the so-called millimeter wave (MMW) band.

MMWs are not new, and are already found in such applications as airport scanners, automotive collision avoidance systems and perimeter surveillance radar security systems. However, the rapid expansion of 5G highspeed wireless systems across the globe “will produce a more ubiquitous presence of MMW in the environment,” the authors noted.

The review prompted the Committee on Man and Radiation (COMAR) of the Institute of Electrical and Electronics Engineers (IEEE) to issue this statement:

“While we acknowledge gaps in the scientific literature, particularly for exposures at millimeter-wave frequencies, [we judge] the **likelihood of yet unknown health hazards** at exposure levels within current limits to **be very low, if they exist at all.”**

COMAR’s consensus statement was issued to counter an **increase in alarming claims** that people and wildlife are suffering strange and **unusual health effects from 5G technology.**

“This **misinformation** together with activist websites expressing even more ominous consequences of 5G — ranging from cancer induction to being responsible for the current coronavirus pandemic — has **created** substantial and **unnecessary** **public anxiety**,” said Jerrold T. Bushberg of the University of California, Davis School of Medicine and vice-chair of COMAR.

Here are the three main reasons why **experts agree** that health **harm** from 5G exposure appears **unlikely**:

In contrast to lower-frequency fields, the MMW band **does not penetrate** **beyond** the outer layer of the skin and so deeper **tissues** are not exposed or heated. Tissue heating is the primary potentially harmful effect of exposure to radiofrequency (RF) fields.

The introduction of **5G** is **unlikely** to **change** overall **levels of RF exposure**. People will continue to receive the most RF exposure due to the “uplink” from their own cell phones and other wireless devices — as they do now — and not from transmission from base stations.

RF exposures from cellular base stations, including 5G stations, will remain small and well below current **international** exposure **standards** and guidelines **in nearly all locations** accessible to the public.

“Exposures may be higher near base station antennas, but wireless carriers are still obligated legally to ensure that transmitting facilities comply with regulatory limits,” the authors noted. “Issues related to compliance are quite possible in countries that have adopted ‘precautionary’ limits that are considerably lower than those in internationally accepted guidelines and standards.”

However, overall **exposure is expected to be lower with 5G** than with 4G base stations because 5G makes more **efficient use of transmitter power** that can steer signals toward specific users. “Since the 5G beam will exist only while communicating with a user, the longterm time-averaged exposure levels will also be lower,” the authors wrote.

“[S]o long as exposures remain below established guidelines, the research results to date do not support a determination that adverse health effects are associated with RF exposures, including those from 5G systems,” according to the COMAR statement.

The experts did acknowledge limitations in the current body of evidence on possible health and safety effects of 5G exposure and identified key areas for further research, including high-quality studies of the biological effects of MMW.

“So far, no comprehensive surveys of environmental 5G signals have been conducted; few 5G networks are presently in operation, and those are largely demonstration projects transmitting at less than full capacity,” the authors wrote. “Nevertheless, the designs of 5G networks are constrained by the same requirements that apply to previous generations of cellular systems: to provide a signal that is strong enough to be useful within a given cell but not so strong as to cause interference to users in nearby cells. Consequently, on this basis alone, one can expect that **exposures** from 5G networks will **not differ greatly** from those associated with present generation networks.”

**The radiation emitted by 5G systems is not harmful to the human DNA**

**NCI, 2022;** The National Cancer Institute coordinates the United States National Cancer Program and is part of the National Institutes of Health, which is one of eleven agencies that are part of the U.S. Department of Health and Human Services. “Cell Phones and Cancer Risk” 03/10/2022 https://www.cancer.gov/about-cancer/causes-prevention/risk/radiation/cell-phones-fact-sheet

Why has there been concern that cell phones may cause cancer?

There are two main reasons why people are concerned that cell (or mobile) phones might have the potential to cause certain types of cancer or other health problems: Cell phones emit radiation (in the form of radiofrequency radiation, or radio waves), and cell phone use is widespread. Even a small increase in cancer risk from cell phones would be of concern given how many people use them.

Brain and central nervous system cancers have been of particular concern because hand-held phones are used close to the head and because ionizing radiation—a higher energy form of radiation than what cell phones emit—has been found to cause some brain cancers. Many different kinds of studies have been carried out to try to investigate whether cell phone use is dangerous to human health.

However, the **evidence** to date suggests that cell phone use **does not cause** brain or other kinds of **cancer** in humans.

Is the radiation from cell phones harmful?

Cell phones emit radiation in the radiofrequency region of the electromagnetic spectrum. Second-, third-, and fourth-generation cell phones (2G, 3G, 4G) emit radiofrequency in the frequency range of 0.7–2.7 GHz. Fifth-generation (5G) cell phones are anticipated to use the frequency spectrum up to 80 GHz.

These frequencies **all fall in the nonionizing range of the spectrum,** which is low frequency and low energy. The energy is too low to damage DNA. By contrast, ionizing radiation, which includes x-rays, radon, and cosmic rays, is high frequency and high energy. Energy from ionizing radiation can damage DNA. DNA damage can cause changes to genes that may increase the risk of cancer.

The NCI fact sheet Electromagnetic Fields and Cancer lists sources of radiofrequency radiation. More information about ionizing radiation can be found on the Radiation page.

The human body does absorb energy from devices that emit radiofrequency radiation. The **only** consistently **recognized biological effect** of radiofrequency radiation absorption in humans that the general public might encounter is heating to the area of the body where a cell phone is held (e.g., the ear and head). However, that heating is **not sufficient** to measurably increase core body temperature. There are no other clearly established dangerous health effects on the human body from radiofrequency radiation.

**Has** the incidence of brain and central nervous system **cancers** changed during the time cell phone use **increased**?

**No**. Investigators have studied whether the incidence of brain or other central nervous system cancers (that is, the number of new cases of these cancers diagnosed each year) has changed during the time that cell phone use increased dramatically.

These **studies found**:

* **stable incidence rates** for adult gliomas in the United States (1), Nordic countries (2) and Australia (3) during the past several decades
* stable incidence rates for pediatric brain tumors in the United States during 1993–2013 (4)
* stable incidence rates for acoustic neuroma (5), which are nonmalignant tumors, and meningioma (6), which are usually nonmalignant, among US adults since 2009

In addition, **studies** using cancer incidence data have tested different scenarios (simulations) determining whether the incidence trends are in line with various levels of risk as reported in studies of cell phone use and brain tumors between 1979 and 2008 (7, 8). These simulations showed that many risk changes reported in case-control studies were not consistent with incidence data**, implying that biases and errors in the study** may have distorted the findings.

Because these studies examine cancer incidence trends over time in populations rather than comparing risk in people who do and don’t use cell phones, their ability to observe potential small differences in risk among heavy users or susceptible populations is limited. Observational/epidemiologic studies—including case–control and cohort studies (described below)—are designed to measure individual exposure to cell phone radiation and ascertain specific health outcomes.

### 5G Bad---AT: Radiation---2AC

#### 5G is fine---radiation isn’t radioactivity.

Paul Lee et al 20 (Paul Lee is a UK Partner and the Global Head of Research for the technology, media, and telecommunications (TMT) industry at Deloitte. 12-7-2020, "5g health risks debunked," Deloitte Insights, <https://www2.deloitte.com/us/en/insights/industry/technology/technology-media-and-telecom-predictions/2021/5g-radiation-dangers-health-concerns.html>) //billy

What has led to this high level of concern about 5G’s health impacts? It may have its roots in a simple confusion of terminology.

Radiation is commonly assumed to involve radioactivity, but this is not necessarily the case. The confusion arises because the words “radiation” and “radioactivity” have been conflated, a confusion that has persisted since the dropping of the Hiroshima and Nagasaki nuclear bombs in 1945. As a result of these events, as well as incidents at several nuclear power plants in the 75 years since, the term “radiation” has often mistakenly become associated with destruction on a massive scale. In a similar vein, “radiation”—in reality, radioactivity—is also associated with cancer, reinforcing the word’s connotation of mortal peril.

The point here is that radiation is not inherently radioactive. The literal definition of radiation is merely any process by which an object (from a human to a radiator to a star) emits energy (whether heat, light, or radioactive particles), which then travels through a medium (such as the air or hot water) and is absorbed by another object (a human body, a frying pan, a steam engine, or anything else). Radiation thus spans multiple everyday processes to which most people do not give a moment’s consideration. In our daily lives, most of us are regularly exposed to multiple types of radiation, most commonly in the form of sunlight.

By this definition, 5G does generate radiation, but at very safe levels, and none of it is radioactive radiation. 5G base stations and phones, and the frequency ranges within which 5G operates, are very likely to be operating well within safe parameters in 2021 and throughout 5G’s lifetime, which may extend to two decades. Radiation within these parameters does not significantly raise the risk of cancer. It also does not weaken the immune system, and thus has not contributed to the spread of COVID-19.

## AT: China Good

### China Good---2AC

#### China’s military rise will drive aggression and war in every theatre.

Gertz ’20 [Bill; February 20; National Security Correspondent, guest lecturer at the Federal Bureau of Investigation, the Central Intelligence Agency, and the National Defense University at Fort McNair; Washington Times, “China's military buildup, global ambitions on collision course with U.S., Pentagon official warns,” <https://www.washingtontimes.com/news/2020/feb/20/chad-sbragia-warns-xi-jinping-china-military-build/>]

China’s decades long military buildup now poses a threat to U.S. security not just in Asia but also around the globe, and a confrontation with China could emerge at one of several flashpoints, a senior Pentagon official warned Thursday.

Chad Sbragia, deputy assistant defense secretary for China, told a congressional commission that Beijing’s buildup of missiles, warships, aircraft, space weaponry and cybercapabilities has accelerated under President Xi Jinping. He described it as “one of the most ambitious military modernization efforts in recent history.”

“In most of the potential flashpoints in the Indo-Pacific region — the Taiwan Strait, the South China Sea, the Senkaku Islands or the Korean Peninsula — the United States may find itself in a military crisis with China,” Mr. Sbragia told a hearing of the congressionally created United States-China Economic and Security Review Commission. He said the challenge posed by Chinese military and economic expansion requires a Cold War-type response.

While not a replica of the standoff with the Soviet Union in the Cold War, the China threat is “equally as consequential and therefore merits the same concentration of effort as put forth in the past,” he said.

China’s military now boasts 2 million personnel in uniform. The Chinese navy, after decades of building large numbers of warships, is now the world’s largest in terms of total assets, he said.

“China’s military is fielding an increasingly formidable array of ballistic and cruise missiles, modern fighter aircraft, autonomous systems, and a suite of cyber and space capabilities, postured to deny the U.S. military access to the Indo-Pacific theater if called upon,” Mr. Sbragia said.

Military power projection efforts are also linked to China’s expanding economic might through such programs as Mr. Xi’s Belt and Road Initiative and military-civilian fusion. China’s single overseas military base in Djibouti, on the Horn of Africa, is just the beginning of a global basing structure to match the U.S. military’s reach, U.S. officials say.

“In other words, it is not a matter of whether the [People’s Liberation Army] intends to establish another military base overseas, but when and how they plan to do it,” Mr. Sbragia said.

“The implications of China’s military modernization are profound. This is a long-term challenge that will require sustained funding and strategic planning to address …,” Mr. Sbragia said. “There is no zero-cost solution to global competition with China.”

Global ambitions

The Capitol Hill hearing also included witnesses who revealed how Chinese military power is expanding globally and could help spread the ruling Communist Party’s authoritarian model. Isaac B. Kardon, a professor at the Naval War College, said the PLA navy could use a network of Chinese commercial ports for logistics in projecting military power. Chinese companies, he noted, own or operate 94 ports around the world, including the ports at either end of the Panama Canal.

“The [Chinese navy] depends on commercial ports to support its growing operations overseas,” he said.

Mr. Kardon cited an unidentified PLA officer who was quoted as saying of the Pakistani port of Gwadar that “the food is already on the plate. We’ll eat it whenever we want to.”

Beijing also has set as a goal the reunification of Taiwan with the mainland by 2049, the 100th anniversary of the rise to power of Mao Zedong’s communists.

By 2035, China plans to deploy a high-technology force with modernized weapons and command and control systems to be able to follow Mr. Xi’s guidance to “fight and win wars.”

Mr. Sbragia said China outlined its goals in a 2019 military white paper that called for the People’s Liberation Army to “safeguard China’s overseas interests” by such means as building “offshore forces” and overseas bases. Chinese military strategists justify the expansion by saying the PLA will be “fulfilling international obligations” to secure the global commons and that Beijing will “never threaten any other country or seek any sphere of influence.”

In the Arctic, China is deploying civilian research organizations that could be used for a military presence.

Taiwan and the South China Sea are prime flashpoints for a direct U.S.-clash, Mr. Sbragia said. He was reiterating U.S. complaints that Beijing has “increasingly employed coercive tactics and measures in the South China Sea to deny claimants the legitimate regulation, exploitation and use of maritime natural resources in their exclusive economic zones.”

The Pentagon’s 2018 National Defense Strategy concluded that China is seeking regional hegemony in the Indo-Pacific and “displacement of the United States to achieve global preeminence in the future.”

Defense Secretary Mark Esper has said repeatedly that a rising China is his department’s top security challenge.

A break with the past

The Pentagon testimony breaks with previous intelligence assessments that China’s military ambitions were limited to retaking Taiwan.

The Pentagon’s 2003 annual report to Congress on the Chinese military concluded that “preparing for a potential conflict in the Taiwan Strait is the primary driver for China’s military modernization.” Subsequent annual surveys emphasized that the buildup was limited to Taiwan but noted that China’s military was also interested in taking part in international peacekeeping and humanitarian operations.

Few of the reports suggested that China had global ambitions to achieve military dominance, as conservative military analysts have argued for years.

Spokesmen for the National Intelligence Council and Defense Intelligence Agency had no immediate comments on the shifting arguments.

Retired Navy Capt. Jim Fanell, a former Pacific Fleet intelligence director, said Mr. Sbragia’s testimony was encouraging.

“Even as short as five years ago, the U.S. intelligence community’s conventional wisdom held that the PRC’s leaders were primarily focused on ‘domestic concerns’ of regime survival or enacting military modernization for regional purposes in order to resolve territorial disputes within the ‘first island chain,’” said Capt. Fanell, referring to the island stretching north to south close to China’s east coast.

“Despite this all-to-common failure to recognize the PRC’s strategic intentions, the fact is the PRC has and continues to build a naval force that if left unchallenged will not only be sailing the seven seas, as it is today, but will increasingly be able to achieve sea control in the global maritime commons as early as 2030, and potentially even sea superiority by 2049,” he said.

Capt. Fanell said the institutional bias to underestimate China’s strategic intentions and PLA modernization and global operations should lead to updates of the language of the 2018 national defense statement, deeming China a strategic adversary or enemy rather than a strategic competitor.

Rick Fisher, a China military analyst, said a small community of skeptics and conservatives can claim vindication with Mr. Sbragia’s testimony, which echoes what they have been saying for over two decades: that an unconstrained China will become a global threat to America.

“Conservatives have also long warned that China’s ambitions go well beyond simply taking over Taiwan,” Mr. Fisher said. “What China will try to do to Taiwan is simply the template for how it will eventually threaten every other democracy.”

#### Tech leadership's enables proper defense against a host of existential threats.

Knipfer ’17 [Cody; Policy Associate at PoliSpace, M.A. Candidate in the Space Policy Institute at George Washington University; A Really Cool Blog, “On the Nature of Science and Technology Power,” <http://www.reallycoolblog.com/on-the-nature-of-science-and-technology-power/>]

Indeed, the United States’ leadership in science and technology has been a historical cornerstone of its capacity for “hard power” force application and projection and economic and societal “soft power.” It buttresses the country’s economic might, enables the modern standards of living of our citizenry, and expands our global cultural and normative reach.[ii] Equally so, the power of science and technology has been decisive in the context of national security. As President Truman noted in 1945, while urging Congress to create a Department of National Defense, “no aspect of military preparedness is more important than scientific research.” [iii] Through discoveries, technological innovation, and the capacity to develop ideas into deployable weapons, systems, and concepts, the United States has arrived at its modern-day military advantage and superiority.[iv]

To that end, science and technology may be considered key elements of the United States’ comprehensive national power – fundamentals of the country’s strength vis-à-vis competitors. Yet science and technology alone cannot ensure any country’s continued security, prosperity, or hegemony; far from operating in a vacuum, science and technology are constantly evolving to address changing domestic and international circumstances and threats. To reap advantage from science and technology, especially in their national security application, a country must continually innovate to tackle contemporary developments and anticipate future ones. This poses a considerable challenge, the solution to which extends beyond advanced engineering and research.

To explore these notions, this essay, particularly interested in the application of science and technology toward national security ends, examines the United States’ recent employment of security-related technologies. From this, it explores the attributes of science and technology power and the similarities and differences between science and technology power and other forms of national power such as the economic and diplomatic. Looking at the relative importance of science and technology in the United States today and likely significance in the coming future, it lays out a series of policy recommendations that may guide policymakers as they make decisions that impact the direction of the country’s scientific and technological course.

Employment of – and Challenges Facing – National Security-Related Technology

Recognizing the vital role that technology played in winning World War Two, along with the emerging threat of Soviet technological competitiveness, the United States established in the war’s wake an extensive infrastructure to support national security science and technology efforts. This provided foundation and catalyst for the development of military capabilities and tools needed to meet the challenges of the Cold War and the modern day: the nuclear triad, intelligence-gathering and cyber infrastructure, space-based radar and communications systems, advanced precision-guided munitions, and integrated command and control, along with myriad other assets.[v]

These technologies have seen extensive use in contemporary military conflicts. The wars in the Balkans and the Gulf saw the ever-increasing use of position, navigation, and timing assets such as GPS to provide precise and reliable information to the warfighter and direct precision-guided weaponry.[vi] Targeted airstrikes and weapons such as the long-range cruise missile have allowed for far more rapid, responsive, and accurate strikes than those of the past while substantially reducing collateral damage. Combat drones and unmanned aerial vehicles, innovations emblematic of the “War on Terror,” enable the warfighter to engage adversaries and conduct reconnaissance while safely remaining away from the front lines of the battlefield. Stealth aircraft, using a range of advanced technologies that reduce reflections and emissions, have helped pilots conduct sorties while evading detection.[vii]

Technology abets the United States’ security beyond warfighting. Advanced cyber capabilities – encryption, for example – seek to defend the networks which control the country’s power, transit, and water infrastructure from malicious hacks and crippling denial of service.[viii] Technologies capable of detecting harmful biological and chemical agents guard the country against potentially devastating attack by non-state actors.[ix] Increasingly sophisticated monitoring and surveillance technology enables the government to globally track and work to counter criminal activity, terrorist organizations, and other developments which threaten the country’s safety.[x]

Crucially, though, the United States’ contemporary application of national security systems has also demonstrated the inherent challenges of innovation and the limitations of technology. Despite advanced military hardware, principally designed to fight large-scale conventional wars against Cold War-era foes, the United States military had to “catch up” and react to unconventional tactics, such as roadside bombs and sniper attacks, employed against it in the Iraq and Afghanistan wars. Though decidedly outnumbered and outgunned, enemy combatants effectively countered the United States’ asymmetric technological advantage through guerilla warfare, propaganda, and exploiting collateral damage that advanced weapons systems created – doctrines which the United States’ technology did not anticipate and was unprepared or unsuited to counter.[xi] Likewise, despite the sophistication of the United States’ homeland security technologies, the government has struggled to prevent incidents of domestic terrorism such as mass shootings, often characterized by the use of simple, off-the-shelf equipment.[xii]

Meanwhile, in reaction to the United States’ present-day technological superiority, competitive foreign powers such as Russia and China are heavily investing in hardware and capabilities in the cyber and military realms specifically designed to counter the United States’ technological strengths and exploit its demonstrated vulnerabilities. The technological capabilities underlying the United States’ comparative military advantage are now proliferating to an increasing number of state and non-state actors, including potential adversaries, leveling the military “playing field.”[xiii]

The Attributes of National Security Science and Technology Power

From this, several key attributes and characteristics of science and technology as a form of national power can be identified. Foremost is the capacity for technology and science to be a significant, occasionally decisive, enhancer of a country’s military strength against enemies. Countries which develop innovative military technologies which effectively counter an adversary’s offenses or defensives, or against which an adversary has no means to protect itself, find themselves disproportionately advantaged on the battlefield. Indeed, technologies which upend dominant “status quo” warfighting paradigms – such as, historically, the introduction of the chariot, the tank, or nuclear weapons – are poised to significantly disrupt and reorder the geopolitical and military balance of power.[xiv]

To that end, science and technology power, particularly in the national security sphere, is developed and sustained through the adaption to, and more so through the anticipation of, revolutionary changes in military affairs, doctrine, and hardware. As Lieutenant Colonel Scott Stephenson noted in the influential “The Revolution in Military Affairs,” “those slow to adapt to military revolutions… are likely to suffer painful results. When the pace of change accelerates, the militaries that anticipate and adapt are likely to gain a massive advantage over potential enemies who are less agile.”[xv] That agility is, in large part, borne from innovations in science and the development of new technologies which lead to unanticipated, and therefore difficult to counter, doctrines.

A defining characteristic of science and technology power, then, is the continual quest for states to match, counter, and out-compete the technology of their adversaries. This continuing interplay between technology and national power, characterized by the sustained technological evolution and described often as an “offset,” has been a key focus for national security-related research and development throughout the Cold War and into the present. The United States’ deployment of nuclear weapons, for example, offset the numerical advantage held by the Soviet Union’s land forces in the early Cold War. Soviet parity in nuclear weapons catalyzed the development of guided weapon and integrated command and control as a counter, focusing on accuracy of targeted weapons systems independent of range.[xvi] The United States’ capacity to offset Soviet technology through innovative developments – and the Soviet bankruptcy borne from military expenditure that came as a corollary – was an important factor in maintaining a generally peaceful stable of power along with the country’s ultimate triumph in the Cold War. In the present-day, China and Russia’s focus on countering the systems and technologies which currently provide the United States’ military asymmetry is emblematic of this “offset” approach to science and technology power.

Paradoxically, however, national security-related technology in the present day has become as great an equalizer as it has historically been a separator of actors’ strengths. Technological superiority in the present may provide the United States’ unrivaled military strength, especially against foes (historically, state actors with large conventional forces) for which its national security technologies anticipated countering. Yet as the example of the Iraq and Afghani insurgencies amply demonstrated, technological superiority coupled with innovation focused on addressing hypothetical future battlefields may not be adequate to oppose or defeat all actors or all forms of warfare, regardless of the level of their sophistication.

Indeed, advanced technologies may be entirely vulnerable to actors utilizing doctrines with simple technologies that nonetheless exploit their weaknesses, as was the case with sophisticated – and expensive – American vehicles being destroyed by crude, homemade IEDs. Technology itself also creates weaknesses; the United States’ progressing economic and social reliance upon interconnected networks, for example, makes the country more vulnerable to potentially crippling attack. Despite advanced American cybersecurity technologies and techniques, non-state actors have still proven themselves capable of infiltrating, attacking, and even denying use of American cyber capabilities; considering recent trends, this vulnerable seems likely to continue, if not worsen.[xvii]

It may be that an attribute of science and technology power, borne more from the focus and perceptions of the technologists, theorists, and military leadership that employ it than from science and technology itself, is that it obscures other factors which equally dictate important developments in military, international, and geopolitical affairs. Political upheaval, social change, and economic development can change warfare dramatically, for example – and have nothing to do with “offset” strategies or war-room predictions of possible enemies’ future high-tech military hardware. As a product of the military-industrial complex that emerged in the Cold War United States to sustain continued technological development, Americans tend to be acutely – perhaps overly – sensitive to technological innovation among competitors and potential rivals. Fears during the Cold War and contemporary discussions of the “Third Offset” paint pictures of emerging, potential, and fanciful enemy weapon systems – which military planning and technology development was and is oriented toward countering.[xviii] This fixation on solutions entailing engineering and technological complexity blinds the national security technology apparatus to external trends that could definitively impact the future course of war – such as the collapse of the Soviet Union leaving the United States with a high-tech military and warfighting doctrine unsuited for the military pressures and asymmetric nature of counterinsurgency; the rise of radical terrorism with ideological underpinnings that condone unconventional guerilla tactics such as suicide bombings, which had great effect against high-tech targets; or the continuing crisis where lone-wolf gunmen using off-the-shelf rifles can commit massacres despite the government’s highly complex and pervasive surveillance and monitoring technology.

Similarities and Differences to Other Forms of National Power

With these attributes in mind, a comparison can be drawn between science and technology power and other forms of power which constitute a country’s comprehensive strength, such as the economic and diplomatic. Regarding the economic, science and technology power is similar in that the development of science and technology is driven by the same forces as economic growth. Like new economic products, services, and methods of operation, science and technology power relies upon the ingenuity of human actors predicting and anticipating future trends, possibilities, and human behavior. Innovation, iteration, and competitiveness are fundamental catalysts for the continued evolution and growth of both. The rapid proliferation and subsequent use of innovative technologies across the world quickly equalizes both the national security advantage and the economic advantage they provided their inventor.

Economic power, like national security technology, is a key element of a country’s warfighting capability – industrial might, strength in quality production, and capable infrastructure are crucial facets of a country’s ability to mobilize and project force. A fundamental difference between economic power and science and technology power, however, is competition. While economies naturally compete, there is incentive for states to specialize in the economic product or service most suited for it – their comparative advantage. Competing economies are not actively incentivized to counter the economic specialization of their rivals. With science and technology power for national security use, however, states decidedly hope to actively and explicitly counter the relative advantage of their adversaries.

Like diplomatic power, science and technology has a “soft power” element; other states and their societies may be influenced or compelled to action by the might, prestige, or cultural and technological hegemony of a country in possession of highly advanced and capable technologies.[xix] Diplomatic power occasionally experiences the same issue of science and technology policy in being blinded to unpredicted or external trends in the social, cultural, and economic spheres. The power of diplomacy, for example, did not anticipate and struggled to deal with the cultural, social, and political circumstances that led to a breakdown of order in post-invasion Iraq; just as national security technology was unprepared for the guerilla warfare of the Iraqi insurgency. Diplomatic power and science and technology power differ, though, in the fields of innovation and evolution. Whereas the military regime is constantly evolving and occasionally being upended by revolutions in security technology and associated doctrine, the Westphalian diplomatic order has remained largely similar through centuries – even as it has grown gradually more complex and interconnected. States do not tend seek to outcompete each other in the diplomatic sphere through revolutionary new approaches to diplomacy; negotiations, sanctions, deals, bi- and multilateral agreements, and the like have remained consistent “doctrines” employed by states in their dealings with international friends and foes.

Science and Technology Power’s Present and Future Importance

To return to Vannevar Bush’s assertion over half a century ago, science and technology is crucially important for a states’ economic growth and prosperity, the wellbeing of its citizens, and national security. This remains absolutely the case today. Despite the challenges facing innovation in the face of unanticipated adversaries and the proliferation of advanced, equalizing technologies among adversarial states and non-state actors, science and technology provides the United States’ unrivaled levels of security and military hegemony.

With the appearance of significant global challenges – refugee crises, environmental degradation, the possible emergence of a bi- or multi-polar world characterized by states with rough or equal technological parity, to name a few – the future importance of science and technology power cutting across all aspects of national security will undoubtedly redouble. Science and technology and its application as an element of the United States’ national power will need to be directed to address these challenges. While the exact characteristics that will define domestic and foreign national security technologies of the future – not to mention the economic and social – remain uncertain, the United States cannot afford to permit its current technological advantage to slip. Indeed, as revision states such as China continue to develop their technologies to directly counter the United States’ capabilities, it will likely become an imperative for the country to more actively engage in and support the development of innovative new security technologies and doctrines – lest, as history would suggest, the international order again be upended.

### China Good---Tech Leadership---2AC

#### Causes extinction---uncontrolled risks from emerging tech cause rapid shifts in strategic stability and misuse---American dominance is key.

Jain **’20** [Ash; 2020; Senior fellow with the Scowcroft Center for Strategy and Security, M.S. in Foreign Service and J.D. from Georgetown University; et al.; “Present at the Re-Creation: A Global Strategy for Revitalizing, Adapting, and Defending a Rules-Based International System,” <https://www.atlanticcouncil.org/wp-content/uploads/2019/10/Present-at-the-Recreation.pdf>]

The system must also be adapted to deal with new issues that were not envisioned when the existing order was designed. Foremost among these issues is emerging and disruptive technology, including AI, additive manufacturing (or 3D printing), quantum computing, genetic engineering, robotics, directed energy, the Internet of things (IOT), 5G, space, cyber, and many others. Like other disruptive technologies before them, these innovations promise great benefits, but also carry serious downside risks. For example, AI is already resulting in massive efficiencies and cost savings in the private sector. Routine tasks and other more complicated jobs, such as radiology, are already being automated. In the future, autonomous weapons systems may go to war against each other as human soldiers remain out of harm’s way.

Yet, AI is also transforming economies and societies, and generating new security challenges. Automation will lead to widespread unemployment. The final realization of driverless cars, for example, will put out of work millions of taxi, Uber, and long-haul truck drivers. Populist movements in the West have been driven by those disaffected by globalization and technology, and mass unemployment caused by automation will further grow those ranks and provide new fuel to grievance politics. Moreover, some fear that autonomous weapons systems will become “killer robots” that select and engage targets without human input, and could eventually turn on their creators, resulting in human extinction. The other technologies on this lisgt similarly balance great potential upside with great downside risk. 3D printing, for example, can be used to “make anything anywhere,” reducing costs for a wide range of manufactured goods and encouraging a return of local manufacturing industries.61 At the same time, advanced 3D printers can also be used by revisionist and rogue states to print component parts for advanced weapons systems or even WMD programs, spurring arms races and weapons proliferation.62 Genetic engineering can wipe out entire classes of disease through improved medicine, or wipe out entire classes of people through genetically engineered superbugs. Directed-energy missile defenses may defend against incoming missile attacks, while also undermining global strategic stability.

Perhaps the greatest risk to global strategic stability from new technology, however, comes from the risk that revisionist autocracies may win the new tech arms race. Throughout history, states that have dominated the commanding heights of technological progress have also dominated international relations. The United States has been the world’s innovation leader from Edison’s light bulb to nuclear weapons and the Internet. Accordingly, stability has been maintained in Europe and Asia for decades because the United States and its democratic allies possessed a favorable economic and military balance of power in those key regions. Many believe, however, that China may now have the lead in the new technologies of the twenty-first century, including AI, quantum, 5G, hypersonic missiles, and others. If China succeeds in mastering the technologies of the future before the democratic core, then this could lead to a drastic and rapid shift in the balance of power, upsetting global strategic stability, and the call for a democratic- led, rules-based system outlined in these pages.63

The United States and its democratic allies need to work with other major powers to develop a framework for harnessing emerging technology in a way that maximizes its upside potential, while mitigating against its downside risks, and also contributing to the maintenance of global stability. The existing international order contains a wide range of agreements for harnessing the technologies of the twentieth century, but they need to be updated for the twenty-first century. The world needs an entire new set of arms-control, nonproliferation, export-control, and other agreements to exploit new technology while mitigating downside risk. These agreements should seek to maintain global strategic stability among the major powers, and prevent the proliferation of dangerous weapons systems to hostile and revisionist states.

### China Good---AT: No Race---2AC

#### China's a digital revisionist. Their tech pursuit is to dominate the global order.

Polyakova ’20 [Alina; 12/15/20; President and CEO of the Center for European Policy Analysis, Ph.D. and M.A. in Sociology from the University of California Berkeley; held numerous fellowships, including at the National Science Foundation, the Woodrow Wilson International Center for Scholars, the Social Science Research Council, and the Fulbright Foundation, Founding Director for Global Democracy and Emerging Technology at the Brookings Institution. Previously, she served as Director of Research for Europe and Eurasia at the Atlantic Council; Eileen Donahoe; J.D. from Stanford Law School, Ph.D. in Ethics and Social Theory from the University of California Berkeley, Executive Director at the Global Digital Policy Incubator; "A Transatlantic Effort to Take on China Starts with Technology," https://cepa.org/a-transatlantic-effort-to-take-on-china-starts-with-technology/]

China’s digital authoritarian model is ambitious. The CCP’s commitment to technological dominance is manifest in its long-term investment strategy. Artificial intelligence (AI) is a focal point because it enables innovation and supremacy in so many other fields. In 2019, China made clear its desire to be the world’s leading AI superpower by 2030,4 with a rough plan to have caught up with the United States by 2020, to surpass the United States by 2025, and to dominate globally in AI industries by 2030.5 The immensity of the regime’s investment in other emerging technologies is staggering, with no less than 16 different “Manhattan Project”-scale initiatives in fields as varied as quantum computing, cryptography, 5G, facial recognition, and genomics.6

China has experimented with and deployed ground-breaking repressive digital technology, most notably against the Uighur minority in Xinjiang. An unprecedented system of mass surveillance monitors the movement of people, phones, and vehicles to detect behavior that merits investigation or detention. This techno-totalitarian system is being extended to other parts of China as well as exported across the world.

Countries as varied as Zimbabwe, Uzbekistan, Pakistan, Kenya, and the United Arab Emirates have bought Chinese surveillance technology.7 Many others have received training in topics like proactive censorship, or “public opinion guidance.” China also exports digital information infrastructure, such as Huawei’s 5G telecommunications systems, under the guise of the Belt and Road Initiative (BRI). These deals create long-term leverage. Even nominally private Chinese companies are obligated by law to provide unquestioning, immediate, and confidential support to the country’s intelligence and security agencies. As U.S. Sen. Mark Warner (D-VA) noted, “any supposedly safe Chinese product is one firmware update away from being an insecure Chinese product.”8

On the diplomatic front, China has made huge efforts to dominate multilateral bodies and agendas in pursuit of regulatory and normative dominance.9 Chinese nationals now lead four of the 16 U.N. agencies, including the International Telecommunications Union (ITU), the United Nations Industrial Development Organization (UNIDO), the International Civil Aviation Organization (ICAO), and the Food and Agriculture Organization (FAO). In its latest push to coopt multilateral institutions, China has led an effort, together with Russia and Saudi Arabia, to place a more pliant head of the U.N. Human Rights Council (UNHRC) and undermine the consensus candidate favored by democracies.10

China recognized very early that it could have significant influence if it sought out leadership roles at tech standard-setting bodies. It adopted an aggressive strategy to push for first-mover advantage for its protocols that can provide a powerful edge to its businesses and sway the global tech community to adopt its protocols for emerging technologies.11 Furthermore, China recently secured a commitment from 14 other countries in the Regional Comprehensive Economic Partnership (RCEP) trade agreement not to challenge its Great Firewall and other digital restrictions. The RCEP is the largest trade pact in world. It cements China’s central role in global supply chains, particularly in high tech. By flexing its economic muscles to gain international political influence, China is winning the global narrative battle about cyber sovereignty and the advantages of its techno-authoritarian model of governance over the U.S.-led democratic one. This brings not only political benefits but significant long-term advantages to Chinese tech firms.

China has even succeeded in normative realms like the UNHRC, where a Chinese representative gained a seat on the influential Consultative Group, which oversees the selection of candidates for U.N. human rights expert roles.12 As the United States has withdrawn from the UNHRC and the EU has been preoccupied with its own problems, China was able to convince the majority of delegations at the council to support declarations that its use of technology in both Xinjiang and Hong Kong are consistent with human rights principles.13 In his speech to the 2020 U.N. General Assembly meeting, Chinese President Xi Jinping positioned China as a responsible stakeholder in the international system, while criticizing “major countries” for not doing enough to contribute — a critique long directed by the United States against China. Xi also announced that China will set up a “U.N. Global Geospatial Knowledge and Innovation Center” and an “International Research Center of Big Data for Sustainable Development Goals” as part of the U.N.’s 2030 Agenda for Sustainable Development,14 positioning China as a hub for international collaboration on technology.

### China Good---AT: Peaceful 5G---2AC

#### China is a techno-nationalist---they’ll use 5G offensively.

Oertel ’20 [Janka; April 4; Director of the Asia Programme at the European Council on Foreign Relations; [Issue 1: Future NATO: Adapting to New Realities](https://www-tandfonline-com.proxy.lib.umich.edu/toc/rwhi20/95/1), “V. NATO’s China Challenge,” p. 67-80]

Techno-Nationalism

As underscored by Evan Feigenbaum, of the Carnegie Endowment for International Peace, for more than a decade China’s current policies have not been new. Instead, they are deeply rooted ‘in old strategies, policies, practices, and predilections, as well as deeply held ideologies about the relationship between technology and national power’.[9](https://www-tandfonline-com.proxy.lib.umich.edu/doi/full/10.1080/02681307.2019.1731211) China’s techno-nationalism describes the relationship as ‘intrinsically strategic’ and focused on military and civilian progress since the 1950s.[10](https://www-tandfonline-com.proxy.lib.umich.edu/doi/full/10.1080/02681307.2019.1731211) Investment in research and development is dominated by a focus on capabilities. Nominally private Chinese technology companies have been at the forefront of driving China’s innovation ecosystem from 5G to facial recognition and other applications supported by artificial intelligence (AI) and the collection of data. Technologies developed by entrepreneurs from Beijing to Shenzhen – with the help of transfer of know-how from international companies seeking to enter the Chinese market, or through actual indigenous innovation and sometimes through outright theft of intellectual property – are often inherently dual use in nature.[11](https://www-tandfonline-com.proxy.lib.umich.edu/doi/full/10.1080/02681307.2019.1731211) This holds especially true in the realms of AI, quantum computing, or drone and satellite technology. China has not completed the translation of these technologies into military capabilities, and although the ‘Revolution in Military Affairs with Chinese Characteristics’, as it is termed in the 2019 White Paper, is well under way, the conclusion in the official document remains that the ‘PLA still lags far behind the world’s leading militaries’ when it comes to modern, information technology-driven warfare.[12](https://www-tandfonline-com.proxy.lib.umich.edu/doi/full/10.1080/02681307.2019.1731211) Given China’s high ambitions, it is important to pay close attention to Chinese technological developments across the board; in Europe especially, the concerns have too often focused merely on the commercial economic dimension and not on potential or actual military applications.

### China Good---AT: Smart Cities---2AC

#### US opposition and data protection destroy Chinese “Smart City” development

Rosas 21 (Alexander Rosas, reporter for “The China Guys” have spent their professional and academic careers learning to decode China, 8-26-2021, "What To Know About China's Smart Cities and How They Use AI, 5G, and IoT," China Guys, https://thechinaguys.com/china-smart-cities-development/, DOA: 7-11-2022//Smarx Ahsan)

Challenges To China’s Smart City Development

US Opposition

While China moves ahead developing its smart cities, the companies behind them could face headwinds should they try to export the technologies. In a report by the US-China Economic and Security Review Commission, it notes that China has become a global leader in smart cities initiatives and elevated the importance of smart cities to a national strategy. It poses a challenge to US-led smart city initiatives due to the sheer amount of support and capital surrounding Chinese-led projects. However, the US is unlikely to import Chinese technologies given its belief that their data sharing protocols could inadvertently expose core US infrastructure to backdoor vulnerabilities and aid Chinese intelligence.

Protecting Data While Building Cities of the Future

After decades of funneling capital into science and technology research, China is starting to see how transformative its investments in this industry can be. Between the capabilities of the national champions that it grew and Beijing’s own investments in smart city technologies, it is likely that the majority of China’s urban areas will become highly interconnected comparatively early. Additionally, the integration of AI and big data in transportation and government services will surely aid in the overall economic development of China’s cities.

However, while the Chinese government is likely to continue its public-private partnerships with domestic tech giants to keep technologies in the hands of the private sector, it is unlikely that many nations in the West will readily import them – a response likely to become a new focal point in regards to smart city technologies between the US and China.  
AT: Smart Cities Bad

## AT: Smart Cities Bad

### Smart Cities---List---2AC

#### 5G innovation enables new smart cities – that’s key to solve disease, pollution, warming, and resource consumption

Costa ’21 [Estevao, 7-27-2021, "The Smart Cities of Tomorrow Enabled by 5G and IoT," CENGN, <https://www.cengn.ca/information-centre/innovation/smart-cities-enabled-by-5g-iot/>, St. Mark’s, AM]

For this reason, the future of smart cities is only as great as the technology that enables them. 5G represents a critical turning point in the evolution of smart cities. With its high-speed, low-latency, and higher capacity wireless connectivity, 5G handles a massive number of connections. This major leap in network speed and capacity allows industries to catch up with innovation, making it practical to deploy emerging technologies such as mass IoT deployments, Artificial Intelligence (AI), and Quantum Computing into our businesses and everyday life.

Benefits of 5G versus 4G

4G’s speed and capacity brought us to where we are today regarding mobile applications, navigation, and video. 4G is genuinely seen as the generation connecting man-to-machine with the smartphone and tablet.

However, 5G boasts a 100x increase in traffic capacity and network efficiency, a 10x decrease in end-to-end latency, and speeds over 600 times faster than the typical 4G speeds (Source: Canadian Wireless Telecommunications Association). That is why many see 5G as the machine-to-machine generation of technology, which warrants no human interaction; machines take actions according to sensor data.

The advanced connectivity features of 5G, such as high bandwidth and low latency fuel the improved machine-to-machine communication leading cities into the new era of IoT-enabled applications that improve services across the industry, including healthcare, transportation, safety, energy management, and many public services.

As technology advances, cities encounter many opportunities in which innovative solutions can reduce strains and improve sustainability.

Smart City Technologies and their Impact on Quality of Life

People may not be aware, but we incorporate smart technologies seamlessly into our daily lives, in every aspect and for the better. Some may acknowledge the impact smart home technologies have made, such as Amazon Alexa or Google’s whole portfolio of smart speakers, lights, cameras, apps, and tools.

These innovations are just the beginning and have already improved convenience, cost of living, and even safety, regarding our homes and daily routine. And, like someone’s house, the city can be optimized with smart technologies to improve all facets of life, including:

Safety

Health

Environment

Urban mobility

Living in a Safer and Smarter Urban Environment

Public safety is a primary target of smart cities, looking to improve life for citizens, the government, and law enforcement by reducing crime and improving emergency response times. For example, a McKinsey Global Institute study points out that smart technologies could help reduce crime by 30 to 40 percent and lead to 20 to 35 percent faster response times for emergency services (Source: McKinsey and Company).

Of course, technology alone won’t eradicate crime and guarantee safety, but it can contribute to more efficient use of resources to prevent and respond to threats. The Next Generation 911 (NG911) is just one example of a technology initiative that focuses on improving public safety. NG911 aims to disrupt the current 9-1-1 response system in place and find better ways to put citizens in contact with emergency responders. This includes working with voice, image, video, and text through digital channels, leveraging IoT and fast networks instead of the traditional analog phone lines used today.

Smart surveillance solutions, real-time crime mapping, and traffic signal pre-emption are other examples that enable authorities to track crime more efficiently and respond to them quicker. Police work driven by data offers citizens more security, fairness in authority accessibility and provides the city consistent emergency coverage according to necessity (Source: McKinsey and Company).

Integrating Health Tech into the City

Typically, the larger the city, the more difficult it is to manage because of environmental impact, logistics, and the sheer number of people. However, health technologies are increasingly being incorporated into municipalities to improve public wellness.

With faster networks connecting professionals, patients can schedule consultations via online video instead of an in-person appointment. For low-income communities, telemedicine is a lifesaver, cutting down on high transportation costs and allowing short-staffed health professionals to save time and see patients more often. This technology is already becoming more common to monitor patient conditions and alert physicians when an intervention is warranted. Perhaps the next step will be to use connectivity to measure individual health and the wellness of a whole urban population.

To properly account for a city population’s health and be ready for unexpected issues, officials can use data and analytics to track key indicators. For example, the community’s primary health issues, hotspots for an outbreak, groups with high-risk profiles, and optimize health campaigns and interventions with precision. This includes messages about vaccination, flu shots, and sanitation.

Smart Cities are Good for the Environment

Growing urban centres have led to increased energy consumption, pollution, and waste, threatening sustainability, especially concerning the environment. However, eco-friendly mobility solutions, dynamic energy and water pricing and management, and air quality sensors can help reduce the environmental impact.

Electric vehicles are becoming more popular by the minute due to their low carbon footprint. Even local transportation is taking note as electric scooters and bikes – also known as micromobility fleets – are another option to drive sustainability in urban centres. Micromobility fleets encourage sharing, alleviate public transport systems for short distances, and lead to a 51% decrease in urban carbon emissions (Source: EY).

Smart cities are already finding ways to implement e-scooters and bikes to make sense for end-users. Enabled by IoT, micromobility fleet apps connect pedestrians in need of transportation with fleet operators and city transit systems to ensure they choose the most efficient method of mobility available. Beyond sustainability, all parties receive an influx of rich data insights concerning transport usage and traffic around the city.

Energy and water consumption tracking is another tool that reduces consumption and increases conservation efforts. Using IoT sensors deployed in meters allows real-time messages to be sent to residents showing them how much energy they’ve used. As a result, incentivize reduced consumption and pave the way for reward programs that encourage more environmentally friendly behaviour. Additionally, the city can deploy sensor technology and artificial intelligence to detect and predict where there might be leaks or defects in water pipes, which can save millions of dollars in resource waste and damages needing repair (Source: United States Environmental Protection Agency).

In terms of data collection, air pollution sensors and analytics help municipal governments identify points of heavy carbon emissions and their causes. This information can then be acted on, sharing data in real-time to take proactive measures, preventing a hike in pollutant concentration rather than waiting until pollution peaks. An example would be incorporating sensor technology and automation into manufacturing processes, allowing for system-wide data analysis. That will determine which manufacturing process produces the most significant carbon footprint and can be optimized towards a more eco-friendly alternative.

### Smart Cities---Disease---2AC

#### 5G-enabled smart cities solves disease

Costa ’21 [Estevao, 7-27-2021, "The Smart Cities of Tomorrow Enabled by 5G and IoT," CENGN, <https://www.cengn.ca/information-centre/innovation/smart-cities-enabled-by-5g-iot/>, St. Mark’s, AM]

Integrating Health Tech into the City

Typically, the larger the city, the more difficult it is to manage because of environmental impact, logistics, and the sheer number of people. However, health technologies are increasingly being incorporated into municipalities to improve public wellness.

With faster networks connecting professionals, patients can schedule consultations via online video instead of an in-person appointment. For low-income communities, telemedicine is a lifesaver, cutting down on high transportation costs and allowing short-staffed health professionals to save time and see patients more often. This technology is already becoming more common to monitor patient conditions and alert physicians when an intervention is warranted. Perhaps the next step will be to use connectivity to measure individual health and the wellness of a whole urban population.

To properly account for a city population’s health and be ready for unexpected issues, officials can use data and analytics to track key indicators. For example, the community’s primary health issues, hotspots for an outbreak, groups with high-risk profiles, and optimize health campaigns and interventions with precision. This includes messages about vaccination, flu shots, and sanitation.

#### Future pandemics cause nuclear war

RECNA, Research Center for Nuclear Weapons Abolition, Nagasaki University (RECNA), Asia Pacific Leadership Network (APLN) & Nautilus Institute (2021), ’21, Pandemic Futures and Nuclear Weapon Risks: The Nagasaki 75th Anniversary pandemic-nuclear nexus scenarios final report, Journal for Peace and Nuclear Disarmament, 4:sup1, 6-39, DOI: 10.1080/25751654.2021.1890867

The relationship between pandemics and war is as long as human history. Past pandemics have set the scene for wars by weakening societies, undermining resilience, and exacerbating civil and inter-state conflict. Other disease outbreaks have erupted during wars, in part due to the appalling public health and battlefield conditions resulting from war, in turn sowing the seeds for new conflicts. In the post-Cold War era, pandemics have spread with unprecedented speed due to increased mobility created by globalization, especially between urbanized areas. Although there are positive signs that scientific advances and rapid innovation can help us manage pandemics, it is likely that deadly infectious viruses will be a challenge for years to come. The COVID-19 is the most demonic pandemic threat in modern history. It has erupted at a juncture of other existential global threats, most importantly, accelerating climate change and resurgent nuclear threat-making. The most important issue, therefore, is how the coronavirus (and future pandemics) will increase or decrease the risks associated with these twin threats, climate change effects, and the next use of nuclear weapons in war.5

Today, the nine nuclear weapons arsenals not only can annihilate hundreds of cities, but also cause nuclear winter and mass starvation of a billion or more people, if not the entire human species. Concurrently, climate change is enveloping the planet with more frequent and intense storms, accelerating sea level rise, and advancing rapid ecological change, expressed in unprecedented forest fires across the world. Already stretched to a breaking point in many countries, the current pandemic may overcome resilience to the point of near or actual collapse of social, economic, and political order. In this extraordinary moment, it is timely to reflect on the existence and possible uses of weapons of mass destruction under pandemic conditions – most importantly, nuclear weapons, but also chemical and biological weapons. Moments of extreme crisis and vulnerability can prompt aggressive and counterintuitive actions that in turn may destabilize already precariously balanced threat systems, underpinned by conventional and nuclear weapons, as well as the threat of weaponized chemical and biological technologies. Consequently, the risk of the use of weapons of mass destruction (WMD), especially nuclear weapons, increases at such times, possibly sharply. The COVID-19 pandemic is clearly driving massive, rapid, and unpredictable changes that will redefine every aspect of the human condition, including WMD – just as the world wars of the first half of the 20th century led to a revolution in international affairs and entirely new ways of organizing societies, economies, and international relations, in part based on nuclear weapons and their threatened use. In a world reshaped by pandemics, nuclear weapons – as well as correlated non-nuclear WMD, nuclear alliances, “deterrence” doctrines, operational and declaratory policies, nuclear extended deterrence, organizational practices, and the existential risks posed by retaining these capabilities – are all up for redefinition.

A pandemic has potential to destabilize a nuclear-prone conflict by incapacitating the supreme nuclear commander or commanders who have to issue nuclear strike orders, creating uncertainty as to who is in charge, how to handle nuclear mistakes (such as errors, accidents, technological failures, and entanglement with conventional operations gone awry), and opening a brief opportunity for a first strike at a time when the COVIDinfected state may not be able to retaliate efficiently – or at all – due to leadership confusion. In some nuclear-laden conflicts, a state might use a pandemic as a cover for political or military provocations in the belief that the adversary is distracted and partly disabled by the pandemic, increasing the risk of war in a nuclear-prone conflict. At the same time, a pandemic may lead nuclear armed states to increase the isolation and sanctions against a nuclear adversary, making it even harder to stop the spread of the disease, in turn creating a pandemic reservoir and transmission risk back to the nuclear armed state or its allies.

In principle, the common threat of the pandemic might induce nuclear-armed states to reduce the tension in a nuclear-prone conflict and thereby the risk of nuclear war. It may cause nuclear adversaries or their umbrella states to seek to resolve conflicts in a cooperative and collaborative manner by creating habits of communication, engagement, and mutual learning that come into play in the nuclear-military sphere. For example, militaries may cooperate to control pandemic transmission, including by working together against criminal-terrorist non-state actors that are trafficking people or by joining forces to ensure that a new pathogen is not developed as a bioweapon.

To date, however, the COVID-19 pandemic has increased the isolation of some nuclear-armed states and provided a textbook case of the failure of states to cooperate to overcome the pandemic. Borders have slammed shut, trade shut down, and budgets blown out, creating enormous pressure to focus on immediate domestic priorities. Foreign policies have become markedly more nationalistic. Dependence on nuclear weapons may increase as states seek to buttress a global re-spatialization6 of all dimensions of human interaction at all levels to manage pandemics. The effect of nuclear threats on leaders may make it less likely – or even impossible – to achieve the kind of concert at a global level needed to respond to and administer an effective vaccine, making it harder and even impossible to revert to pre-pandemic international relations. The result is that some states may proliferate their own nuclear weapons, further reinforcing the spiral of conflicts contained by nuclear threat, with cascading effects on the risk of nuclear war.

Developing Pandemic-nuclear Nexus Scenarios

How might the COVID-19 pandemic (and future pandemics) create new opportunities or challenges for governments, civil society, and market actors to reduce nuclear risk and resume nuclear disarmament? And how might those challenges and opportunities emerge in Northeast Asia, in particular?

#### Diseases cause extinction

Ord, Senior Research Fellow at Oxford, ‘20 [Toby; reporter for the Guardian; 3-6-2020; "Why we need worst-case thinking to prevent pandemics"; Guardian; https://www.theguardian.com/science/2020/mar/06/worst-case-thinking-prevent-pandemics-coronavirus-existential-risk]

The world is in the early stages of what may be the **most deadly pandemic** of the **past 100 years**. In China, thousands of people have already died; large outbreaks have begun in South Korea, Iran and Italy; and the rest of the world is bracing for impact. We do not yet know whether the final toll will be measured in thousands or hundreds of thousands. For all our advances in medicine, humanity remains much **more vulnerable** to pandemics than we would like to believe. To understand our vulnerability, and to determine what steps must be taken to end it, it is useful to ask about the very worst-case scenarios. Just how bad could a pandemic be? In science fiction, we sometimes encounter the idea of a pandemic so severe that it could cause **the end of civilisation,** or even of **humanity itself.** Such a risk to humanity’s entire future is known as an **existential risk.** We can say with certainty that the novel coronavirus, named Covid-19, does not pose such a risk. **But could the next pandemic?** To find out, and to put the current outbreak into greater context, let us turn to the past. In 1347, death came to Europe. It entered through the Crimean town of Caffa, brought by the besieging Mongol army. Fleeing merchants unwittingly carried it back to Italy. From there, it spread to France, Spain and England. Then up as far as Norway and across the rest of Europe – all the way to Moscow. Within six years, the Black Death had taken the continent. Tens of millions fell gravely ill, their bodies succumbing to the disease in different ways. Some bore swollen buboes on their necks, armpits and thighs; some had their flesh turn black from haemorrhaging beneath the skin; some coughed blood from the necrotic inflammation of their throats and lungs. All forms involved fever, exhaustion and an intolerable stench from the material that exuded from the body. There were so many dead that mass graves needed to be dug and, even then, cemeteries ran out of room for the bodies. The Black Death **devastated Europe.** In those six years, between a **quarter and half of all Europeans were killed**. The Middle East was ravaged, too, with the plague killing about **one in three Egyptians and Syrians**. And it may have also laid waste to parts of central Asia, India and China. Due to the scant records of the 14th century, we will never know the true toll, but our best estimates are that somewhere between **5% and 14% of all the world’s people were killed**, in what may have been the **greatest catastrophe** humanity has seen. The Black Death was not the only biological disaster to scar human history. It was not even the only great bubonic plague. In AD541 the plague of Justinian struck the Byzantine empire. Over three years, it **took the lives** of roughly **3% of the world’s people.** When Europeans reached the Americas in 1492, the two populations exposed each other to completely novel diseases. Over thousands of years, each population had built up resistance to their own set of diseases, but were extremely susceptible to the others. The American peoples got by far the worse end of the exchange, through diseases such as measles, influenza and, especially, smallpox. During the next 100 years, a combination of invasion and disease took an immense toll – one whose scale may never be known, due to great uncertainty about the size of the pre-existing population. We can’t rule out the loss of more than 90% of the population of the Americas during that century, though the number could also be much lower. And it is very difficult to tease out how much of this should be attributed to war and occupation, rather than disease. At a rough estimate, as many as 10% of the world’s people may have been killed. Centuries later, the world had become so interconnected that a truly global pandemic was possible. Towards the end of the first world war, a devastating strain of influenza, known as the 1918 flu or Spanish flu, spread to six continents, and even remote Pacific islands. About a third of the world’s population were infected and between 3% and 6% were killed. This death toll outstripped that of the first world war. Yet even events like these fall short of being a threat to humanity’s long-term potential. In the great bubonic plagues we saw civilisation in the affected areas falter, but recover. The regional 25%-50% death rate was not enough to precipitate a continent-wide collapse. It changed the relative fortunes of empires, and may have substantially altered the course of history, but if anything, it gives us reason to believe that human civilisation is likely to make it through future events with similar death rates, even if they were global in scale. The Spanish flu pandemic was remarkable in having very little apparent effect on the world’s development, despite its global reach. It looks as if it was lost in the wake of the first world war, which, despite a smaller death toll, seems to have had a much larger effect on the course of history. The full history of humanity covers at least 200,000 years. While we have scarce records for most of these 2,000 centuries, there is a key lesson we can draw from the sheer length of our past. The chance of human extinction from natural catastrophes of any kind must have been very low for most of this time – or we would not have made it so far. But could these risks have changed? Might the past provide false comfort? Our population now is a **thousand times greater** than it was for most of human history, so there are vastly **more opportunities** for new **human diseases to originate.** And our farming practices have created **vast numbers of animals** living in **unhealthy conditions** within **close proximity to humans**. This increases the risk, as many major diseases originate in animals before crossing over to humans. Examples include HIV (chimpanzees), Ebola (bats), Sars (probably civets or bats) and influenza (usually pigs or birds). We do not yet know where Covid-19 came from, though it is very similar to coronaviruses found in bats and pangolins. Evidence suggests that diseases are crossing over into human populations from animals at an increasing rate. **Modern civilisation** may also make it much easier for a **pandemic to spread**. The higher density of people living together in cities **increases the number of people** each of us may infect. Rapid **long-distance transport** greatly increases the **distance pathogens can spread**, reducing the **degrees of separation** between any two people. Moreover, we are no longer divided into isolated populations as we were for most of the past 10,000 years. Together these effects suggest that we might expect **more new pandemics**, for them to **spread more quickly**, and to reach a **higher percentage** of the **world’s people**. But we have also changed the world in ways that offer protection. We have a healthier population; improved sanitation and hygiene; preventative and curative medicine; and a scientific understanding of disease. Perhaps most importantly, we have public health bodies to facilitate global communication and coordination in the face of new outbreaks. We have seen the benefits of this protection through the dramatic decline of endemic infectious disease over the past century (though we can’t be sure pandemics will obey the same trend). Finally, we have spread to a range of locations and environments unprecedented for any mammalian species. This offers special protection from extinction events, because it requires the pathogen to be able to flourish in a vast range of environments and to reach exceptionally isolated populations such as uncontacted tribes, Antarctic researchers and nuclear submarine crews. It is hard to know whether these combined effects have increased or decreased the existential risk from pandemics. This uncertainty is ultimately bad news: we were previously sitting on a powerful argument that the **risk was tiny**; now **we are not.** We have seen the indirect ways that our actions aid and abet the origination and spread of pandemics. But what about cases where we have a much more direct hand in the process – where we deliberately use, improve or create the pathogens? Our understanding and control of pathogens is very recent. Just 200 years ago, we didn’t even understand the basic cause of pandemics – a leading theory in the west claimed that disease was produced by a kind of gas. In just two centuries, we discovered it was caused by a diverse variety of microscopic agents and we worked out how to grow them in the lab, to breed them for different traits, to sequence their genomes, to implant new genes and to create entire functional viruses from their written code. This progress is continuing at a rapid pace. The past 10 years have seen major qualitative breakthroughs, such as the use of the gene editing tool Crispr to efficiently insert new genetic sequences into a genome, and the use of gene drives to efficiently replace populations of natural organisms in the wild with genetically modified versions. This progress in biotechnology seems unlikely to fizzle out anytime soon: there are no insurmountable challenges looming; no fundamental laws blocking further developments. But it would be optimistic to assume that this uncharted new terrain holds only familiar dangers. To start with, let’s set aside the risks from malicious intent, and consider only the risks that can arise from well-intentioned research. Most **scientific and medical research** poses a negligible risk of harms at the scale we are considering. But there is a small fraction that uses **live pathogens** of kinds that are known to **threaten global harm**. These include the agents that cause the **Spanish flu, smallpox, Sars and H5N1 or avian flu**. And a small part of this research involves **making strains** of these pathogens that pose **even more danger** than the natural types, increasing their **transmissibility**, lethality or resistance to vaccination or treatment. In 2012, a Dutch virologist, Ron Fouchier, published details of an experiment on the recent H5N1 strain of bird flu. This strain was extremely deadly, killing an estimated **60% of humans it infected** – far beyond even the Spanish flu. Yet its inability to pass from human to human had so far **prevented a pandemic**. Fouchier wanted to find out whether (and how) H5N1 could naturally develop this ability. He passed the disease through a series of 10 ferrets, which are commonly used as a model for how influenza affects humans. By the time it passed to the final ferret, his strain of H5N1 had become directly transmissible between mammals. The work caused fierce controversy. Much of this was focused on the information contained in his work. The US National Science Advisory Board for Biosecurity ruled that his paper had to be stripped of some of its technical details before publication, to limit the ability of bad actors to cause a pandemic. And the Dutch government claimed that the research broke EU law on exporting information useful for bioweapons. But it is not the possibility of misuse that concerns me here. Fouchier’s research provides a clear example of well-intentioned scientists enhancing the destructive capabilities of pathogens known to threaten global catastrophe. Of course, such experiments are done in secure labs, with stringent safety standards. It is highly unlikely that in any particular case the enhanced pathogens would escape into the wild. But just how unlikely? Unfortunately, we don’t have good data, due to a lack of transparency about incident and escape rates. This prevents society from making well-informed decisions balancing the risks and benefits of this research, and it limits the ability of labs to learn from each other’s incidents. Security for highly dangerous pathogens has been **deeply flawed**, and remains insufficient. In 2001, Britain was struck by a devastating outbreak of foot-and-mouth disease in livestock. Six million animals were killed in an attempt to halt its spread, and the economic damages totalled £8bn. Then, in 2007, there was another outbreak, which was traced to a lab working on the disease. Foot-and-mouth was considered a **highest-category pathogen**, and required the highest level of biosecurity. Yet the virus escaped from a **badly maintained pipe**, leaking into the **groundwater at the facility**. After an investigation, the **lab’s licence was renewed** – only for **another leak to occur two weeks later.** In my view, this track record of escapes shows that even the **highest biosafety level** (BSL-4) is **insufficient for working on pathogens** that pose a risk of global pandemics on the scale of the Spanish flu or worse. Thirteen years since the last publicly acknowledged outbreak from a **BSL-4 facility** is not good enough. It doesn’t matter whether this is from insufficient standards, inspections, operations or penalties. What matters is the poor track record in the field, made worse by a lack of transparency and accountability. With current BSL-4 labs, an **escape of a pandemic pathogen** is only a **matter of time.**

### Smart Cities---Warming---2AC

#### 5G-enabled smart cities solve pollution and warming

Costa ’21 [Estevao, 7-27-2021, "The Smart Cities of Tomorrow Enabled by 5G and IoT," CENGN, <https://www.cengn.ca/information-centre/innovation/smart-cities-enabled-by-5g-iot/>, St. Mark’s, AM]

Smart Cities are Good for the Environment

Growing urban centres have led to increased energy consumption, pollution, and waste, threatening sustainability, especially concerning the environment. However, eco-friendly mobility solutions, dynamic energy and water pricing and management, and air quality sensors can help reduce the environmental impact.

Electric vehicles are becoming more popular by the minute due to their low carbon footprint. Even local transportation is taking note as electric scooters and bikes – also known as micromobility fleets – are another option to drive sustainability in urban centres. Micromobility fleets encourage sharing, alleviate public transport systems for short distances, and lead to a 51% decrease in urban carbon emissions (Source: EY).

Smart cities are already finding ways to implement e-scooters and bikes to make sense for end-users. Enabled by IoT, micromobility fleet apps connect pedestrians in need of transportation with fleet operators and city transit systems to ensure they choose the most efficient method of mobility available. Beyond sustainability, all parties receive an influx of rich data insights concerning transport usage and traffic around the city.

Energy and water consumption tracking is another tool that reduces consumption and increases conservation efforts. Using IoT sensors deployed in meters allows real-time messages to be sent to residents showing them how much energy they’ve used. As a result, incentivize reduced consumption and pave the way for reward programs that encourage more environmentally friendly behaviour. Additionally, the city can deploy sensor technology and artificial intelligence to detect and predict where there might be leaks or defects in water pipes, which can save millions of dollars in resource waste and damages needing repair (Source: United States Environmental Protection Agency).

In terms of data collection, air pollution sensors and analytics help municipal governments identify points of heavy carbon emissions and their causes. This information can then be acted on, sharing data in real-time to take proactive measures, preventing a hike in pollutant concentration rather than waiting until pollution peaks. An example would be incorporating sensor technology and automation into manufacturing processes, allowing for system-wide data analysis. That will determine which manufacturing process produces the most significant carbon footprint and can be optimized towards a more eco-friendly alternative.

#### Climate crises cause global war and extinction.

Beba Bajalski 20, MM, Consultant at Vortimer Consulting, “Danger of World Conflicts Expansion Due to Climate Change,” UDC 005.334:314.74(4-672EU)”20”, UDC 327.56:551.583, Security Crises in the 21st Century and How to Manage Them: Vol. 1, pp 78-87

Alarming climate change poses a danger to the entire ecosystem of the planet. The aim of this paper is identification of the turning point in civilization existence and world conflicts expansion linked to dangers of climate change. The subject of this paper is exhibited by the methodology based on the general social and scientific experience and with the use of the comparative method. Ecological crisis creates the need for sustainable development. The ecological crisis is caused by excessive exploitation of natural resources and environmental pollution. In the 21st century, humanity is exposed to increasingly pronounced consequences of the endangered ecological balance, as well as to the problems in the social sphere which can altogether lead to global conflicts. The results gained through the analysis of materials indicate that it is of utmost importance that scientific community must be included in the political decison-making process regarding climate change.

1. Ecological security

The term ecological security was introduced by the UN General Assembly, when, at the suggestion of Mikhail Gorbachev, it adopted the “Resolution on International Environmental Security” in 1987 as a reaction to the Chernobyl environmental and human tragedy (Our Common Future 1987, 7). In its report entitled “Our Common Future”, the World Commission on Environment and Development (the so-called Brundtland Commission) proposed that “the whole notion of security as traditionally understood in terms of political and military threats to national sovereignty - must be expanded to include the growing impacts of environmental stress - locally, nationally, regionally, and globally” (Ibid). Author Seyom Brown distinguishes seven world interests considering that the modern understanding of security implies not only national, but also global, world security, which implies the protection and realization of world interests, focused on the needs of humanity “because it spatially encompasses the interests of all peoples and nations on Earth”:

(1) the survival of the human species;

(2) reducing the killing and elimination of others;

(3) the lack of conditions for a healthy life for all people;

(4) protection of civil rights;

(5) respect for the right of peoples and numerous ethnic groups to cultural diversity;

(6) environmental protection - irresponsible attitude towards the natural environment [...] produces consequences in a wider space and over time; often at first glance it is not possible to see how disregard for long-term consequences [...], ultimately endangers the interests of all people and nations [...], and

(7) expanding accountability/responsibility (Brown 1998, 8-10).

It can be concluded that, although Gorbachev introduced the term after the Chernobyl tragedy, 32 years after that terrible event which clearly showed what could happen, the humanity still does not give enough importance to negotiations as a tool for avoiding conflicts and wars, especially taking into consideration the present Atomic era. It has to be underlined that climate change, caused by many negative environmental human activities including hypothetical possibility of an atomic tragedy and the political and global interests of world powers, causees lack of ecological security. Another example of belittling ecological security is the withdrawal of the United States from the Paris Agreement on climate change mitigation in June 2017, as well as their unilateral withdrawal in 2019 from the nuclear agreement with Russia, which has been in force since 1987. Given the threateningly unpleasant increase in conflicts and wars in the 21st century worldwide, which can be observed as the general concept of wars for strategic resources, the ecological security of the entire planet is highly endangered. It can be noted that the ecological security i.e., environmental safety is related to general concept of safety. It concerns the degree of destruction of local and global ecosystems; water shortages, floods; mass and irrational deforestation; environmental pollution and biodiversity depletion. It can be concluded that the conflicts and wars of 21 st century, waged with new and increasingly toxic weapons, threaten life on the planet, and together with the negative changes in the environment caused by new technologies of post-industrial development, lead to the ecological crisis of modern civilization. Thus, taking into consideration opinion of the proponents of the expanded idea of security, any problem related to the environment and the worrying fact of climate change is also a security problem. Author Norman Myers, on the other hand, believes that not all environmental problems lead to a violent conflict, but looking in the long term, a causal link can be found between environmental issues and policy changes (Myers 2004, 3).

Author Thomas Homer-Dixon singles out hypotheses of three groups environmental security threats and challenges:

– the first group is represented by conflicts between states that, at the same time, consider that they have the right to exploit the same natural resources;

– the second group are various migrations of population, which consequently occur due to various environmental disasters and catastrophes in cases when different ethno-religious groups settle in new areas, so there are divisions and conflicts between them, because they do not share the same norms and values;

– the third group of threats refers to the demise of public institutions and internal “social instability”, which can lead to conflicts of unprecedented proportions, and are caused by endangering the population due to disappearance of natural resources, energy and raw materials, environmental pollution, climate change, natural disasters caused by human negligence, etc. (Homer-Dixon 1994, 3-4). Thus, it can be observed that contemporary security threats are caused in high extent by internal conflicts and conflicts between states as well in no lesser extent. In the modern era, the stability and peace of a state can be endangered not only by other states, but by internalstate inefficient management as well.

Author Simić states that Sigmund Freud called the emergence of conflict on the basis of cultural and religious identity within a state “narcissism of small differences” and that the term first appeared in Freud's 1929 work entitled “Civilization and Its Dissatisfaction”, representing the idea that it is precisely the small differences between people who are otherwise similar that form the basis of feelings of alienation and enmity between them (Simić 2002, 49-50). Simić explains that the main consequence that arises from such an internal conflict is the spread of the conflict to nearby, neighboring countries, regions, and even beyond; manifestations of social dangers, endangering something or someone can be unintentional - unconscious or intentional - conscious (Ibid). The author gives an example that technological development is aimed to improve the quality of life, but through inappropriate application, it can lead to endangering the natural basis of human existence on the planet Earth (Ibid). It can be concluded that, eighteen years after the previously mentioned warning, technological development started to be one of the main reasons for rapid climate change and deterioration of ecological security.

This can also be confirmed through the author's Cherry classification, according to which ecological security should deal with maintaining the optimal relationship between organisms, i.e., animal rights issues, the legal status of nature, and the relationship between humans and nature (Cherry 1995, 87). Cherry indicates three kinds of approaches such as:

 The nature-centric, which starts from an understanding of nature as a separate entity and ecology as a science that deals with relations between organisms and their environment.

 The second approach Cheery calls human-centric, and explains that environmental safety is based on a man as a user and controller of nature. The basis for interpreting the environmental safety of this approach are problems related to natural resources, considering the so-called “environmental refugees” and conflicts between people in relation to the environment, as well as the role of international governmental and non-governmental organizations in creating international security through the creation of policies and international law.

 The third approach Cherry considers as being best described as eclectic. It seeks to contribute to a general insight into the phenomenon of environmental safety, taking into account the interdependence between life forms, ecosystems, the social system, individuals and the technical system (Ibid, 87-89).

It can be concluded that there are a lot of threats to ecological security and that they can be observed in two wide groups. The first group of threats is presented by forms and origins of dangers that are out of range of human influence, and the second group of threats lay within the borders of human influences.

Authors Naude and Alcorta warn that “human-induced climate change and its effects on global development is part of the more general challenge of achieving environmental sustainability. It requires a rethink of the process and outputs of production and of distribution and consumption” (Naude and Alcorta 2010). They agree with the opinion expressed by Sachs that “the global economy is literally unsustainable now and cannot absorb further economic and population growth without serious risks of global destabilization – even collapse” (Sachs 2009). It can be concluded that a lot of authors indicate the threats caused by human influences as a major risk for ecological security of the world.

Author Arthur Westing starts from the relationship between people and nature and believes that natural resources are a prerequisite for human well-being and survival (Westing 1989, 129). In his opinion, population growth and the aspiration for the entire population to reach the standard of living of developed countries contributes to the negative impact on the environment, and the struggle for natural resources can lead to conflict (Ibid). Linking the environment and security, in the context of defining human security, he underlines the intertwining of political security, which includes military, economic and social/humanitarian sub-components, and security related to environmental protection (Ibid). Regarding ecological security, it can be observed that it is a new, modern form of security which appeared as a necessity for prevention of environmental threats, with a role to protect the components of the environment which are basic for the survival of living beings. Ecological security calls for encouragement and requirements to involve as many participants as possible in order to implement policies, not only to survive but as well to improve the quality of life of the population and ecology. It can be concluded that, although ecological crisis is one of the most dangerous features of 21st century civilization, political rulers of the world still do not undertake any major globally accepted actions for enforcing ecological security in order to provide survival of living beings and the nature.

2. Climate strike

The climate situation in 2020 is difficult, as shown by the findings of European Climate Change Monitoring Service  Copernicus. The average temperature in January 2020 was 3.1 degrees Celsius higher than the average January temperature, which makes it the warmest in the last four decades (Copernicus 2020). Lauren Fox quotes that the Esperanza Research Center in Antarctica in February 2020 measured a temperature of 18.3°C, the highest temperature ever since 1961, when measurements began there (Fox 2020). Authors Wennersten and Robbins underline that “we are now witnessing the human devastation of the earth” (Wennersten & Robbins 2017, 32). It can be concluded that there is an urgent need for a better model of development for the survival of humanity. Author Miltojevic indicates the grate disadvantage of the new industrial mode of production, concluding that technical progress “deepens contradictions between anthropogenic expansive activities and limited potentials of existing natural resources” (Miltojevic 2002, 254).

Even in a state of strictly individualistic capitalism, such as the United States, it is no coincidence that Benny Sanders appeared in the 2019 presidential race, expressing many actually socialist ideas in his program, such as free health care and education. This fact illustrates the extent of unsustainability of the system, in which both America and all of humanity now exist, in the long run. The idea of sustainability is based on the "triangle of sustainable development", widelyaccepted concept proposed by Munasinghe at the 1992 earth Summit in Rio. This concept includes environmental protection, economic security and social justice, and opposes to a strictly profitable social development strategy, which is global but has led to environmental crisis (Munasinghe 2010, 11).

It can be stated that the 21st century brought up global inequality and a great gap between ultra-rich and other habitants. Specifically, during the year of 2020, marked by COVID-19 pandemic, it leads to great unemployment and austerity and very uneven differentiated regional development in the world. Thus, all of these factors brought social insecurity. The previously described dangerous economic situation causes the lack of environmental protection. Accordingly, the humanity does not properly invest into environment but widely exploit it. It can be stated that all the previously mentioned factors have inexcusable negative effect on environmental security and trigger fundamental damage of people's quality of life which further on may cause risk of conflicts spreading.

It can be observed that the regional development of the entire globe is very uneven. Author Šimleša underlines that the so-called benefits of economic globalization and the rule of the market lead virtually everywhere in the world to reduced funding for social assistance, education and health care, to unfair privatizations and to elimination of the concept of “public good” (Šimleša 2000, 110). It can be concluded that all these factors do not allow implementation of the concept of sustainable development and thus reduce the level of social security, which lead to first climate strike in history.

According to Laville and Watts, Greta Thunberg, climate activist has inspired four million people to the Global Climate Strike on September 20th, 2019, the largest youth environmental protest in history (Laville & Watts 2019). It can be concluded that, although without the decarbonization of the world economy the planet will be destroyed, political circles are not implementing enough international actions in order to cause a global turn towards green economy. Accordingly, the previously mentioned climate strike tries to increase global consciousness regarding ecological security.

3. Climate change as the seed of geopolitical change and danger of world conflicts

Climate change is manifesting itself in an increasing number of natural disasters, affecting the decline of the power of states and endangering world security. The World Bank report for 2018 estimates that Latin America, sub-Saharan Africa and Southeast Asia will generate 143 million climate migrants by 2050 (Kumari Rigaud et al. 2018, 2). China, Taiwan, the Philippines, Malaysia, Brunei and Vietnam are in conflict over the South China Sea resources due to overfishing and water pollution (Fridtjof Nansens Institute 2017). According to Evagelos, conflict situation in the Arctic between the USA (Alaska), Canada, Russia, Norway, Sweden, Finland, Iceland and Greenland are related to climate change, shrinking ice surface of Arctic and conflict for large oil and gas deposits and fish stocks. The Arctic warming is happening twice as fast as anywhere on the Earth (Evagelos 2018). It can be concluded that the rivalry of the Arctic nations also leads to destruction of the fish wealth of the Arctic, leading further to environmental crisis and environmental unsafety, which represents a fruitful seed for conflicts between the Arctic nations. It can be observed that problems that arose in the environment as a consequence of anthropogenic action, led to a different angle of thinking about connection between environmental problems and safety in the end of 20th and in the first two decades of 21st century. The connection between the environment and war conflicts was pointed out through “research on environmental and security issues related to global environmental change, environmental scarcity, degradation and stress, as well as their possible socio-political consequences” (Jovanović Popović 2013, 106). In fact, as the author Bajagić indicates, the growing manifestation of environmental problems contributes to security being defined not only as the protection of the territorial integrity and sovereignty of the state. Moreover, contemporary discussions on security include research into multiple and complex relations and processes between states and within the state (Bajagić 2006, 222). It can be concluded that the said discussions are oriented extensively towards relations between human society and nature. Increasing pressure on natural resources causes demographic, economic and political dangerous conflict changes. Autor Lee indicates: “The seeds of conflict will lie in massive migrations, border tensions and disputes over essential resources” (Lee 2009, 82). “The changing climate has always been a factor in the rise and fall of peoples and civilizations. This phenomenon is often accompanied by conflict ...” (Ibid, 166). Wennersten and Robbins underline that “climate refugees, once thought to be a problem confined to segments of the developing world, are on the verge of becoming a global problem” (Wennersten & Robbins 2017, 32). Although the Paris Climate Agreement entered into force on November 4, 2016, the climate change still contributes to migration due to desertification, rising sea levels, pollution of the oceans, air, land, rainy seasons changes and loss of biodiversity. Environmental protection is not effective. Ecological migrations are evidence to that inefficiency. The UN states that from 2002 to 2012, climate change affected the lives of 4.4 billion people (UNHCR Factsheet 2019). It should be noted that impending disasters are huge migrations of the population due to lack of food, water and land, and frequency of intra-state and inter-state conflicts over resources. Climate change is also affecting the emergence of various epidemics and diseases. Authors Welzer and Camiller (2015) state that “whether wars in the twentyfirst century are directly or indirectly due to climate change, violence has a great future ahead of it. We shall see not only mass migration, but also violent solutions to refugee problems ...” (Welzer & Camiller, 2015, 6). It can be concluded that climate change is a dangerous factor that leads to migration of human population on Earth, and that it is a large precondition for the spread of conflicts.

#### **Air pollution causes extinction**

St. Martin ’22 [Victoria St. Martin, 5-17-2022, "Study Identifies Outdoor Air Pollution as the ‘Largest Existential Threat to Human and Planetary Health’," Inside Climate News, <https://insideclimatenews.org/news/17052022/outdoor-air-pollution-health/>, St. Mark’s, AM]

Since the turn of the century, global deaths attributable to air pollution have increased by more than half, a development that researchers say underscores the impact of pollution as the “largest existential threat to human and planetary health.”

The findings, part of a study published Tuesday in The Lancet Planetary Health, found that pollution was responsible for an estimated 9 million deaths around the world in 2019. Fully half of those fatalities, 4.5 million deaths, were the result of ambient, or outdoor, air pollution, which is typically emitted by vehicles and industrial sources like power plants and factories.

The number of deaths that can be attributed to ambient air pollution has increased by about 55 percent—to 4.5 million from 2.9 million—since the year 2000.

Deaths from ambient air and chemical pollution were so prevalent, the study’s authors said, that they offset a decline in the number of deaths from other pollution sources typically related to conditions of extreme poverty, including indoor air pollution and water pollution.

“Pollution is still the largest existential threat to human and planetary health and jeopardizes the sustainability of modern societies,” said Philip Landrigan, a co-author of the report who directs the Global Public Health Program and Global Pollution Observatory at Boston College.

The report noted that countries with lower collective incomes often bear a disproportionate share of the impacts of pollution deaths, and called on governments, businesses and other entities to abandon fossil fuels and adopt clean energy sources.

“Despite its enormous health, social and economic impacts, pollution prevention is largely overlooked in the international development agenda,” says Richard Fuller, the study’s lead author, who is the founder and CEO of the nonprofit environmental group Pure Earth. “Attention and funding has only minimally increased since 2015, despite well-documented increases in public concern about pollution and its health effects.”

The peer-reviewed study, produced by the 2017 Lancet Commission on Pollution and Health, using data from the 2015 Global Burden of Disease (GBD), found that roughly 1.2 million deaths were attributable to household air pollution (which generally comes from tobacco smoke, household products and appliances); about 1.3 million deaths were attributable to water pollution and 900,000 deaths were attributable to lead pollution.

Pollution's Fatal Toll

All told, the study’s authors wrote, roughly 16 percent of deaths around the world are attributable to pollution, which resulted in more than $4 trillion in global economic losses.

Ambient air pollution can be generated by a range of sources, including wildfires.

### Smart Cities---5G Key---2AC

#### 5G enables smart city creation – security, infrastructure, and communication

Contento ’21 [Marco Contento, 8-13-2021, "5G and the Smart City," Telit, <https://www.telit.com/blog/5g-smart-city/>, St. Mark’s, AM]

Looking at both present and near-future possibilities, let’s explore some 5G smart city applications.

Traffic Management and Analytics

Many cities use or are interested in Intelligent Traffic Systems (ITS), designed to limit congestion on roadways. Such systems monitor traffic and use AI and machine learning to identify patterns and change key elements (e.g., traffic light cycles at certain times of the day) to reduce congestion.

Depending on the system, legacy technology may provide adequate connectivity. Yet if a city wants to stream high-quality video for real-time analysis, 5G’s high bandwidth will help. Some cities in China monitor traffic with video cameras. They use multi-access edge computing (MEC) for video processing and 5G for uplink to the cloud-based analytics engine and data lakes.

Smart Utilities and Metering

5G will have a massive impact on utilities, including infrastructure changes. Today’s smart meters tend to be low-power devices with minimal throughput needs. Smart utilities’ power generation and grids will reap immediate 5G benefits. The utility company needs to synchronize power sources for wind farms to keep the ultimate current generated in phase.

5G will provide dependable connectivity for frequency regulation (i.e., an automatic power adjustment to stabilize and synchronize power to avoid outages). Utility companies looking into and implementing private LTE will have the option to upgrade to private 5G networks for added performance and security.

5G for Public Safety

Most first responder cellular systems such as FirstNet in the U.S. are based on LTE technology. There is early support for a public radio system in 5G. Operators are considering devices for FirstNet on 5G bands. To make this function, designers will need to develop devices to support both technologies. Beyond radio communication, there are multiple potential 5G applications in first responder technology, including:

Connected headsets

Body cams

Augmented reality smart glasses

Vital signs monitors

These devices could benefit from 5G’s higher bandwidth and robust security. 5G can prompt further development of devices to help first responders do their jobs.

Public Transit

Most public transportation sensors monitor the physical position of trains and buses. However, some cities are looking at 5G’s additional benefits. A Swiss company is integrating 5G in their GPS tracking device to provide broadband connectivity for train passengers. Airlines may do this on private and commercial jets to provide onboard connectivity. For automakers, 5G will provide vehicle-to-vehicle and vehicle-to-infrastructure communications to enable autonomous public transportation.

Smart Buildings

Smart buildings present a complex scenario with many possible situations and applications. Older cellular technology may remain dominant for several years, except when it’s inconvenient to install wired connections. In those cases, 5G can be considered.

As 5G becomes available, it will be a natural part of smart building infrastructure. When Rel 17 improves massive IoT and low-power sensor performance and price points, smart buildings will benefit from making the shift. Buildings with temperature sensors to measure heat consumption rely on Wi-Fi connectivity, which can be spotty and cyberthreat vulnerable. In a world where 5G is ubiquitous, data flow from those sensors will become much more dependable and easier to secure.

Autonomous Vehicles

5G will be crucial for the auto industry to enable safe and effective autonomous vehicle operation. Self-driving cars depend on sensor technologies and onboard computers. They must retain constant connectivity with GPS satellites and a tiered cloud-based system. 5G will enable vehicle-to-vehicle communication so self-driving cars can share roadways with one another (and human drivers).

Electric Vehicles

5G will impact the distribution of energy for electric vehicles. Current power networks cannot support vast numbers of electric cars. One possible solution is energy sharing. If a solar-powered charging station is connected to the grid and not in use or not being used to full capacity, it can cogenerate into the grid.

Public Illumination

Smart lighting is another use case that will function well with low-power wide-area network technology for the foreseeable future. This application doesn’t have an immediate need to switch to 5G. However, as 5G infrastructure rolls out, some cities may consider dual-usage smart streetlights to provide light and 5G coverage. We will likely see many dual-use applications incorporating 5G with existing technology to provide improved services.

5G Cybersecurity

Cybersecurity is a legitimate concern for connected smart city devices. With IoT’s lack of regulation and clear security standards, devices can have hardware and software vulnerabilities. City IT officials must choose providers with a proven security track record to ensure security. As it will enable massive numbers of connected devices, 5G will highlight the need for robust security policies. Smart city designers must be vigilant in pursuing secure solutions to offset risks.

While 5G impacts connectivity, it will create space for many innovations to match its capabilities. These innovations will include new devices and software platforms to manage complex analytics. A smart meter might monitor a building’s energy consumption throughout the day and night and adjust prices based on current demand. The meter might then notify the user via the utility’s smartphone app (or interactive screen on the connected thermostat). Diverse smart city applications working in concert will become an integrated system. 5G will enable these additional use cases, enhancing the number of services and escalating their complexity.

### Smart Cities---5G Key---1AR

#### Fully integrated projects fail now – only 5G solves

Castro ’19 [Daniel, Castro is the vice president of the Information Technology and Innovation Foundation (ITIF) and director of the Center for Data Innovation, January 2019; "5G Can Enable Smart Cities — If Policymakers Allow It," GovTech, <https://www.govtech.com/fs/infrastructure/5g-can-enable-smart-cities-if-policymakers-allow-it.html>, St. Mark’s, AM]

Many cities are striving to become “smart” — communities at the forefront of using data, sensors and connected devices to improve government services and residents’ quality of life through analytics and automation. Smart cities promise to deliver notable advances, such as less roadway congestion from smart traffic signals, more effective health and safety inspections with predictive analytics, and more transparency with real-time dashboards showing citizens when to expect the next snowplow or garbage truck to come through their neighborhood.

But for most cities, especially those in the U.S., becoming a fully functioning smart city is a dream still only on the horizon. While many have launched important smart city initiatives, these tend to be one-off projects instead of fully integrated smart city efforts that modernize city governments from top to bottom. Yet comprehensive smart city efforts are necessary to fully extract the value that data analytics can deliver to government.

One step cities can take to come closer to realizing their vision of becoming a smart city is accelerating the deployment of 5G wireless networks. 5G, which offers faster connections, more reliability and greater capacity at lower costs, will enable cities to better connect their infrastructure, devices and people. Moreover, compared to the current 4G standard, 5G offers the capacity to enable additional smart city capabilities, and it will be a prerequisite to enable various high-bandwidth and low-latency smart city applications. For example, 5G will support the wide-scale deployment of connected vehicles communicating with traffic signals to reduce traffic as well as the deployment of large numbers of sensors to measure in real time the safety of infrastructure such as water pipes, highways and buildings.

#### Specifically, 5G security is necessary for smart city development

Park & Shalla ’21 [Sung Jin and Kristi, Park earned her PhD in planning, policy and design at University of California Irvine and is now developing 5G business models for Korean smart cities, Shalla is a member of the Smart City Global Specialist Network with the South Korean government and has 15 years of development experience in smart cities, 10-24-2021, "Get Ready for a 5G Smart City," Smart City Journal, <https://www.thesmartcityjournal.com/en/articles/get-ready-for-a-5g-smart-city>, St. Mark’s, AM]

Security and Data Protection

As we enter the era of dynamic development in smart city infrastructure, the issue of online security looms large on the horizon because so much of our personal information is being housed in digital locations. There are worries that the high level of dependencies on 5G puts cities at a greater risk of hacking. It is in part true in the sense that wireless networks are more vulnerable to cyber-attacks than wired networks. In the case of wireless communications, no physical access is required, and network boundaries are blurred. These attributes tend to allow more unauthorized access opportunities compared with wired networks.

There are approaches that cities can take in order to obtain a secured 5G network. The first is to build a private 5G network - a dedicated closed 5G mobile network that meets location-specific coverage and can be exclusively used only by authorized devices. Secondly, cities can implement technologies and regulations encrypting field-level data. A lot of edge devices or servers have offered data encryption functions. The transmission of encrypted data can minimize 5G network attacks.

Lastly, it is the adoption of quantum cryptographic communication technologies. Quantum’s unique mechanics block any type of cyber-attacks during transmission more effectively than in wired networks, and the deployment of secure 5G communications using quantum cryptography has been tested and being expanded across the world starting from South Korea. In reality, only greenfield cities can design and build a fully secured smart city implementing a private 5G, the data encryption governance of IoT devices, and the application of quantum science. The dominant number of cities is likely to apply only part of the solutions against cyberattacks and gradually implement them. It remains uncertain how to balance cybersecurity worries over 5G and the promise and potential of 5G for smart cities.

### Smart Cities---5G Key---QKD---1AR

#### QKD is key to beat China’s telecom dominance

Xchange ’19 [Quantum Xchange, 5-21-2019, "How QKD Answers Huawei’s Looming Threat to the U.S. Telecom Market," QuantumXC, <https://quantumxc.com/blog/qkd-huawei-telecom-market/>, St. Mark’s, AM]

Whether we like it or not, China’s major telecom provider, Huawei, is infiltrating the global telecom market.

Last week, the Trump administration banned American companies from doing business with Huawei. Shortly after, Google cut ties with the company.

But does the door to potential spying by the Chinese government still remain open?

While some of the biggest domestic telecom firms like AT&T and Verizon Wireless have promised to avoid Huawei equipment in their 5G wireless networks, this doesn’t rule out rural carriers. Huawei also plans to roll out their own operating system next year, meaning reliance on American companies will be negligible.

“We are going to have to figure out a way in a 5G world that we’re able to manage the risks in a diverse network that includes technology that we can’t trust,” Sue Gordon, Deputy to the Director of National Intelligence explained in a recent Washington Post article.

Huawei’s momentum will be hard to stop, and that means we need a better way to encrypt our vital communications. This is the perfect opportunity for quantum telecom, to become part of the solution. Quantum telecom is simply the process of communicating securely over long distances by harnessing the power of quantum physics, through Quantum Key Distribution (QKD).

The Huawei Cybersecurity Threat

Chinese tech giant Huawei was founded in 1987 by a former Chinese People’s Liberation Army officer, with the support of the Chinese government. It has grown to be the second-largest smartphone maker as well as a global leader in 5G wireless networks.

A 2012 US House of Representatives’ report called the company a national security threat, while U.S. intelligence agencies (NSA, CIA, FBI, etc.) have articulated the same cybersecurity concerns, urging U.S. citizens not to use Huawei products and services. Considering that the Chinese government heavily subsidizes the company, the cybersecurity concerns are not unfounded even though Huawei officials strongly deny allegations of any ties to or influence from the Chinese government.

U.S. Efforts to Manage the Threat

Stemming from the concern that Huawei will use its products to spy for China and steal intellectual property, the U.S banned government agencies and contractors from buying Huawei products and services in the latest National Defense Authorization Act (NDAA). In May, the Trump administration also banned U.S. companies from doing business with the Chinese telecom company.

At the same time, the U.S. has been lobbying hard (but rather unsuccessfully) to get our allies to follow suit. So far Australia and New Zealand have taken measures to restrict the use of Huawei products, but England just signed an agreement with the company allowing it to help build “non-core” components of the UK’s 5G infrastructure. Moreover, the European Commission decided recently not to warn European Union member nations against contracting with the company; and NATO likewise chose not to impose a blanket ban on the company for its member nations.

What is the Answer? Developing Technology to Safeguard Our Networks

While Huawei continues spreading through telecom markets overseas, the company is fighting the U.S. ban and has sued the US government, stating that the ban is unconstitutional. Whether it will be successful in fighting that battle remains to be seen, but Huawei’s influence and the threat it poses will remain.

Carriers all over the world are getting ready to move from 4G LTE to 5G this year, promising ultra-fast data speeds and allowing more data to travel on wireless networks. Unfortunately, this also opens the door wider to individuals who want to steal the data off those networks. The challenge will be for U.S. telecom providers to prevent any espionage on foreign 5G networks from reaching into domestic networks.

A quantum communications network like Quantum Xchange’s Phio may just be the answer to that challenge. Quantum Key Distribution (QKD) offers unbreakable encryption of data which will safeguard against the prospect of quantum technological power and its ability to decrypt data; but it could also be applied to the security threat posed by Huawei as 5G networks come online.

We certainly can’t wait to find out what Huawei’s intentions are. The imperative to act now, to manage the risk now, is clear.

# Case---Military

## Mechanics

### Military---2AC

#### NATO cybersecurity standards are key to military 5G.

Piret Pernik 21, Researcher at the NATO Cooperative Cyber Defense Centre for Excellence, Research Fellow at the Internal Centre for Defence and Security; et al., 2021, “Research Report Supply Chain and Network Security for Military 5G Networks,” https://ccdcoe.org/library/publications/research-report-supply-chain-and-network-security-for-military-5g-networks/, RMax, MNOs = Mobile Network Operators

8. Recommendations

8.1. Supply Chain Security

NATO should set trustworthiness criteria for high-risk 5G equipment manufacturers and associated service providers with a view to mitigating malicious intent (such as the insertion of vulnerabilities, interception, or disruptions of supply). In cooperation with the EU, risk assessment and management procedures and the baseline criteria for supply chain and network security should be developed and implemented in cooperation with MNOs (taking into account that untrusted elements also exist in trusted networks). Mitigating supply chain risks requires a close public-private partnership of NATO, national governments, and industry.

MNOs should share information with governments and armed forces regarding security controls of critical network functions (notably, pertaining to soft- and hardware, systems, and products and services) and provide information on the security vetting of personnel who have access to them.

8.2. Network Security

NATO nations should jointly determine appropriate network security levels and add-ons to commercial security controls for military-grade networks and associated services. NATO should determine common criteria for the certification of products and services.

Further research should be encouraged with regard to technical network security challenges, including on how to apply Zero Trust Security principles and respective industry tools, end-to-end encryption for military communications over 5G networks, autonomy and automation for monitoring and detection, and AI-enabled analytics and security.

8.3. Policies and Standards

NATO nations should harmonise national strategies and policies to secure commercial and military 5G networks. NATO should consider developing a strategy and/or roadmap for the development of military 5G use cases, addressing, among other things, interoperability of equipment, services, and the radio frequency spectrum. The roadmap should identify the type of military use cases deployed over commercial networks and deployment scenarios for private (military/defence/NATO) 5G networks.

NATO’s standards development organisation should consider how the current 3GPP standards address the security requirements of the military. NATO nations should certify products, processes, and services associated with 5G technology according to jointly agreed criteria, taking into account the existing certification schemes and assessing their value and sufficiency. Nations should actively participate in standardisation work.

NATO nations should ensure the interoperability of national commercial and military 5G networks.

NATO should consider developing Alliance-wide standards for resilient, reliable, available and secure civilian and military 5G networks and consider military-grade standards for military networks.

8.4. Research, Education, and Training

Further research should explore the opportunities 5G technologies can provide for improving Allied defence and deterrence and the security risks inherent in these networks. Awareness raising concerning risks associated with both public (commercial) and military 5G networks should continue targeting specific training audiences (such as the general public, parliaments, decision-makers in government and industry, and military officers). NATO nations should also commission studies to determine what competence and skills are needed in the armed forces and NATO to enable the deployment of military 5G networks and ensure their security.

Further research is needed into what use cases are feasible and less risky from a security point of view. For example, integrating mission-critical C2 with commercial 5G networks in an armed conflict/combat scenario may be too risky, but the use of commercial 5G networks for uses cases such as predictive maintenance, vehicle platooning, or AR/VR training might be feasible.

NATO nations should invest into network security testing laboratories (such as Estonia’s Cyber Range CR14 5G SA test bed) and encourage cooperation between test beds.

NATO should commission research on practical ways and means to enhance nations’ participation in global standardisation work.

O-RAN should be studied in terms of opportunities to increase security, the interoperability of products, and market diversity, as well as to assess risks emerging from open source technology. O-RAN standards should follow the industry best practices. This research should recommend ways and means to mitigate O-RAN risks.

Further research is also needed on how to establish a 34 NATO-owned and -accredited virtual MNO and e-SIM that NATO nations could use.

8.5. Partnerships

NATO nations should enhance timely information and best-practices-sharing, including risk assessments, concerning commercial and military 5G networks. To this end, nations should establish points of contact and create subject-matter-expert networks in relevant government and armed forces organisations. Similar networks of experts should be created with the participation of universities, research institutions, and industry.

Governments and armed forces should have sufficient visibility of supply chain and network security processes, procedures, and practices used by manufacturers of 5G technology and providers of associated services (such as MNOs and cloud service providers). Armed forces should establish partnerships with commercial service providers and equipment manufacturers that enable them to assess risks and assure the integrity, security, resilience, privacy, and quality of the acquired products, systems, and services throughout their life cycle. 5G network service providers should be encouraged to cooperate with armed forces to access the security controls of RAN, MEC, core network, and other critical functions. MNOs should share confidential information with armed forces on issues such as their 5G risk assessments, security policies and controls, and certification of their network components.

NATO and the EU should set up a regular informal consultation body to jointly assess risks and develop mitigation measures across strategic, technical, and supportive dimensions, building on the EU’s experience with risk assessments and the Toolbox.

Technology can be neutral and value-agnostic in principle, but it rarely is in practice. NATO should counterbalance China’s ambitions to attain global dominance in key EDT by developing like-minded technologies that are trusted, secure, reliable, available and resilient. NATO should support the adoption of this trusted technology globally, while refraining from using authoritarian opponents’ technology that is commonly used undermine democratic values and freedoms.

#### Cybersecurity is key to military 5G.

Robert Spalding 21, former Senior Director of Strategy to the President at the National Security Council, founder and CEO of SEMPRE, retired Air Force Brigadier General, 10/20/2021, "U.S. military must resolve widespread security threats to harden commercial 5G for the warfighter," https://militaryembedded.com/comms/communications/us-military-must-resolve-widespread-security-threats-to-harden-commercial-5g-for-the-warfighter, RMax

The deployment of 5G networks by the U.S. military will be an historic moment for today’s warfighter. From improved C5ISR [command, control, computers, communications, cyber, intelligence, surveillance, and reconnaissance] readiness and geolocation accuracy to more effective enemy engagement and perimeter defense, 5G gear will enable scalable, extremely low-latency, mobile radio platforms and an Internet of Things edge-sensor network that puts the power of real-time AI and machine learning into the hands of the combat soldier. This future state is achievable, but not without confronting a blunt reality: 5G is an open architecture designed for commercial applications and as such suffers from a great many security vulnerabilities. To build a resilient, secure, survivable 5G military communications network, we must first harden and future-proof the COTS [commercial off-the-shelf]-based hardware, software, and firmware that are the foundation of today’s civilian 5G infrastructure.

As commercial 5G service rolls out across the U.S. with the promise of 100 times greater speeds than its 4G predecessor, it’s time to examine how the U.S. military can equip the modern warfighter with an upgrade to today’s outmoded battlefield communications infrastructure.

This is no small feat. 5G was designed by an international coalition of technology companies, with heavy input from state-owned Chinese firms. As an open-source, commercial standard, 5G is riddled with potential security threats, nearly 800 of which have yet to be resolved by the governing 3GPP standards body. Moreover, the uptake of 5G by the warfighter will require the U.S. military to forego a decades-long practice of developing bespoke, incompatible radio hardware and move toward a shared, hardened communications framework.

Communications alignment is a national security imperative

The good news? The overhaul and unification of the military’s communications network is already underway in key areas.

The U.S. Department of Defense (DoD) is committed to its Joint All-Domain Command and Control (JADC2) mission, which according to the Congressional Research Service (CRS), aims to “connect sensors from all military services – Air Force, Army, Marine Corps, Navy, and Space Force – into a single network.” This alone will accelerate the speed of decision-making for the soldier and command-and-control (C2) center, which is an urgently needed component of the U.S.’s National Defense Strategy as it prepares for the emergence of Mach 5+ hypersonic weapons.

The U.S. Air Force is contributing to the JADC2 mission by developing the Advanced Battle Management System (ABMS), a C2 framework that the CRS describes as “using secure cloud environments and new communications methods to allow Air Force and Space Force systems to share data seamlessly using artificial intelligence.” In effect, this is an attempt at integrating a sensor-based Internet of Things (IoT) network that reinvents the conventional, airborne C2 structure by extending the eyes and ears of our warfighters to an intelligent edge.

Just as importantly, a unified communications topology must support the nation’s Nuclear Command and Control System (NCCS), which guides the chain of command in providing the President with information required to authorize (and prevent unauthorized) use of nuclear weapons.

Allure of 5G processing speeds tempered by inherent security risks

The military has long been eager to build a common telecommunications and computing platform that enables new software applications to be adopted at the same speed as the commercial sector – or better yet, harden Android and Apple iOS smartphones for use in the field. At best, however, today’s warfighter is relegated to using the phone’s GPS map function for geolocation, which is often more reliable than their military-issued gear.

5G is the enabling technology that will underpin the military’s digital transformation, but 5G was never designed as a native military radio waveform. This reality presents significant challenges and entails the recognition that more than 60% of what the 3GPP ratified as 4G and 5G standards were developed primarily by state-owned Chinese companies. That raises concerns relative to the influence China may have exercised over an industry standards-making body – and the number of unsecured backdoors and man-in-the-middle vulnerabilities through which classified data can be siphoned or modified.

As a point of reference, a 2019 report released by IoT cybersecurity specialist, Finite State, looked into Huawei Technologies and found that 55 percent of tested Huawei devices had at least one potential backdoor. In its summary of findings, Finite State concluded that “if you include known, remote access vulnerabilities along with possible back doors, Huawei devices appear to be at high risk of potential compromise.”

What a 5G future will look like for the warfighter

The future 5G state we should be working to realize will enable users to harness the power of AI, machine learning, and hundreds of thousands of sensors at the IoT edge. Doing so will give troops real-time intelligence and processing while providing secure battlefield computing and communications using fixed and transportable cellular towers supplemented by vehicle-mounted data center nodes. All of this can be achieved using commercial off-the-shelf (COTS) hardware, software, and firmware, as long as it’s all sufficiently hardened to ensure a secure connection to both the network and computing platform.

So, practically speaking, what would a typical 5G application look like? Let’s consider base security: A lot of what occurs on the battlefield involves establishing and maintaining a security perimeter. We can surmise that 5G-enabled communications technology will enable easy supplementation of the perimeter with field-of-motion and pressure sensors. When activated, those sensors feed into a tower-based alert system that sends out drones to investigate. The drones leverage video streaming and facial recognition, and if a threat is detected, can trigger an automated targeting system. If deployed properly, 5G will enable users to very quickly automate their field operations.

Marry the cell tower and data center node

In a commercial 5G application, a smartphone streaming data sends a signal to a nearby tower, which routes the request to a data center that may be hundreds of miles away. The data is retrieved and sent back through the tower and on to the user. That’s a large threat surface, as was seen with the May 2021 Colonial Pipeline ransomware cyberattack.

A more secure, resilient solution is to co-locate the cell tower and data center and build hundreds of them as part of a distributed, compartmentalized network. Not only does this provide better, more even coverage, but if one tower is compromised the others will continue to send and receive data. In turn, that data is wrapped in purpose-built security layers from the inside out – not as a programming afterthought – and provides the warfighter with a “zero-trust network” that includes encryption, user authentication, sandboxing, behavioral analytics, and other protective measures.

It’s this concept that led to the development of the SEMPRE Tower, which is based on the idea that a hardened, COTS-based 5G telecommunications and computing infrastructure can be adapted by the military to improve collaboration on the battlefield while maintaining a secure, resilient C5ISR [command, control, computers, communications, cyber, intelligence, surveillance, and reconnaissance] framework that can withstand a nuclear electromagnetic pulse (EMP) attack. (Figure 1.)

[Figure 1 omitted]

SEMPRE Towers are currently undergoing advanced field trials with the DoD, Air Force, and Army. As the trials progress, the goal is to reimagine battlefield communications by equipping the war­fighter with a data gateway – and a data sentry – that securely and seamlessly connects them across different military branches with the performance, flexibility, and ease-of-use of a commercial smartphone.

### Military---Ext

#### **NATO 5G networks are vulnerable to cyber threats---NATO risk assessment key.**

Pernik ’21 [Piret; October 2021; Research Fellow at the International Centre for Defence and Security, Researcher at the Cooperative Cyber Defence Centre of Excellence, M.A. in International Relations and European Studies from Central European University, M.A. in Sociology from the Tallinn University Estonian Humanitarian Institute; et al.; "Research Report Supply Chain and Network Security for Military 5G Networks," https://ccdcoe.org/uploads/2021/10/Report\_Supply\_Chain\_and\_Network\_Security\_for\_Military\_5G\_Networks.pdf]

The North Atlantic Council (NAC) recently expressed that ‘cyber threats to the security of the Alliance are complex, destructive, coercive, and becoming ever more frequent.’102 The council affirmed determination ‘to employ the full range of capabilities, as applicable, at all times to actively deter, defend against, and counter the full spectrum of cyber threats, in accordance with international law.’103 Telecommunications, including 5G networks, are also susceptible to cyber threats. This section outlines the supply chain and network security risks related to 5G technology and systems.

The armed forces of NATO nations and NATO command structure need to take into account vulnerabilities, threats and risks related to both public and private 5G networks. Three 5G network deployment models for military use identified in this report come with their own security challenges, which should be understood and assessed.104 While the Research Report focuses on military use cases, it cannot disregard the vulnerabilities, threats and risks associated with commercial 5G networks, because in practice, the military will largely use networks and equipment available commercially. Almost all telecommunication technologies are for dual (i.e. military and civilian) use, and inevitably, there will be interdependencies (and hence, vulnerabilities) across the whole life cycle involving many stakeholders (including third-party suppliers and service providers, such as private companies that own and operate mobile cell towers). Therefore, visibility into the supply chain ecosystem is essential for the military.

The security of 5G networks is a very broad and complex topic, and research on it continues to evolve. Many white papers, research reports, overviews and other studies have been published in this area in the last decade. Several distinct threat taxonomies and categorisations of non-technical and technical 5G security risks have been developed by international and governmental organisations, equipment vendors and technical security researchers. A choice of a specific methodology to assess risks depends on a particular target audience – for example, reports addressed to telecommunication sector experts offer a very detailed description of technical security risks associated to infrastructure, components and interfaces of 5G architecture. In addition, the academic and think-tank literature includes a large body of writings offering overviews for policy-makers and regulators who lack technical knowledge of telecommunications.

In addition to supply chain challenges (including the trustworthiness criteria of vendors) and network security challenges, physical security and electromagnetic inference threats to military use cases must be considered, along with traditional insider threats.105 In case of the deployment of the military 5G network on an expeditionary operation in an armed conflict, electromagnetic interference attacks are likely to impede network connectivity and system capacity. However, those attacks have also been launched in peacetime. 5G networks used for expeditionary operations in high-intensity kinetic conflict must meet the most stringent military security requirements in the areas of resistance to jamming, network resilience, and security.

The armed forces must assume that 5G network infrastructure is vulnerable to cyberattacks from both encryption and resiliency standpoints. The military must be able to operate over untrusted networks or networks, including some untrusted components or insecure interfaces.106 This could mean that the military cannot transfer and store classified data in some 5G networks, even though pilot projects for classified information exist. Needless to say, the fact that a given equipment manufacturer, MNO, or third-party service provider is geographically located in the jurisdiction of an EU or NATO nation does not guarantee that infrastructure, equipment, or services provided by these stakeholders are secure. Even trusted networks with recognised security maturity can be accessed physically, by malicious insiders (such as MNO employees), and through electromagnetic and cyberattack means. In such cases, the NATO nations’ armed forces need to consider what types of information and military functions can be transmitted and stored in public and hybrid 5G networks.

#### Inevitable 5G deployment requires NATO coordination to capitalize on emerging tech.

Andrea Gilli and Francesco Bechis 20 (Affiliate at CISAC and a Researcher at the NATO Defense College in Rome where he works on defense innovation and military transformation. 9-30-2020, "NATO Review," NATO Review, <https://www.nato.int/docu/review/articles/2020/09/30/nato-and-the-5g-challenge/index.html>) /billy

Why it matters?

Four main reasons related to telecommunications underlie the increased attention to 5G. First, telecommunications are broadly speaking an enabling technology, which can drive economic growth across the entire economy. Forecasting models predict for example that 5G networks will add trillions of dollars of economic value to the international economy. Just as 4G unleashed a major wave of technological transformation – from the iPhone and Google.maps to Instagram and Whatsapp via Uber and Snapchat – 5G networks are expected to deliver similar effects. Second, telecommunications are generally dominated by a first-mover advantage: early entrants can accrue enormous economic value, leaving little room for competitors. Actors – from companies to countries – thus have a strong incentive to consolidate their position and maximize economic returns. Third, telecommunications carry a strategic dimension: the speed, quality and quantity of information are crucial for competing in the digital world. Finally, given the centrality information plays in modern economies, telecommunications are widely, and rightly, considered a strategic industry. Companies transfer private, and often sensitive information. Governments share diverse types of data, including classified material.

5G and China

Another important reason that 5G has attracted particular attention is that the leading players in this technology are not Western, Japanese or South Korean companies but rather China-based companies like Huawei and ZTE. Several factors explain the rise of Chinese operators in this domain. One is the expertise and experience they acquired with their failed bid to enter the 3G competition over a decade ago. Following this, the Chinese government launched major public investments in this area and developed a coherent strategy, while private companies conducted research and patented their seminal technologies. Chinese companies also enjoy a competitive advantage, especially when approaching foreign markets on 5G: at home, they can count on a widespread availability of fibre, large deployments of small cells, a higher availability of spectrum in low-frequency bands and the maturity of 4G, as well as an enormous domestic market and low production costs. Chinese, Japanese and South Korean companies have long played an important role in telecommunications markets around the world. In fact, Huawei and ZTE from China as well as Nec (Japan) or Samsung (South Korea) are key suppliers in current 4G networks. However, the role of Chinese companies in 5G communications has a very different connotation. With 5G – involving massive machine-to-machine communications – perimeter cyber defence will no longer be effective as it will be impossible to grant access exclusively to authorised devices. As a result, the risk and potential severity of attacks grow exponentially. Also, the more important role of software in network virtualisation will grant equipment integrators (i.e. potentially Chinese companies) wider and deeper access into network operations (i.e. data), thus raising serious questions about trust and reliability. In other words, changes in technology have severe political implications, especially because Chinese companies have direct political connections to their government, including to the intelligence community. China’s internal big data policy – based on massive surveillance and limited privacy – is at odds with other countries’ systems of values, ethics and law. And finally, Chinese companies have in recent years repeatedly been accused of stealing intellectual property and using cyber-espionage to access proprietary information. Tests on Chinese electronic devices have often also revealed security vulnerabilities, including backdoors that can lead to the direct transfer of data to China.

NATO Allies and 5G

Until last December, NATO had taken no stand on 5G communications. Even after the London Leaders Meeting, no single policy or position has truly emerged. Looking at the Allies’ response, we can identify five main groups: the concerned, the lawmakers, the undecided, the sceptics and the early adopters.

The concerned

To date, the United States is the only NATO country that has taken effective steps to restrict access to its 5G network from Chinese companies like Huawei or ZTE. Importantly, however, the US administration’s ban announced in May 2019 has not yet entered into force due to 90-day extensions that have been renewed four times. Congress has passed some bills with wide bipartisan consensus – such as the so-called “rip and replace act” (signed into law by President Trump in March 2020) – which compel Huawei and other Chinese companies to stick to stricter security controls or, in other cases, support Western companies in the 5G competition. Along the same lines, in May 2020, the U.S. Department of Commerce announced an amendment to its Entity List, subjecting Huawei to individual licensing requirements for exports. By targeting Huawei’s acquisition of semiconductors, the decision aims to curtail severely the company’s competitiveness. Huawei eventually confirmed that such an amendment would put its very survival at stake. Similarly, the U.S. Department of State launched the “5G Clean networks”, a plan for setting a “clean path” for allies of the United States to exclude Chinese vendors from their networks.

The lawmakers

Some Allies, such as Italy, have not placed a ban on Chinese 5G equipment manufacturers but have already committed to stricter regulations. In late 2019, the Italian government approved a law establishing a “National Cyber-Security Perimeter” which in turn introduced more stringent rules and procedures to assess the security of 5G equipment. Germany fits into the same category. Despite a passionate internal debate, the Federal Government is not expected to ban Chinese companies from its 5G network. Deutsche Telekom has already announced that it will continue working with Chinese 5G providers.

The undecided

The positions of some NATO countries have evolved over time, progressively adopting a stricter stance. The Czech Republic signed a joint declaration with the United States on 5G security on 6 May 2020, stating the intent “to strengthen our cooperation on 5G” and determine whether the network is “subject, without independent judicial review, to undue foreign influence”. Similarly, after an initial assessment phase in January 2020, the Greek government slowed the deployment of 5G infrastructure owing to “national security and protection of the country’s critical infrastructure”. The United Kingdom is another example. Initially, in January 2020, the British government announced a 35 per cent cap on Huawei’s participation in the “non-core part” of the 5G network, while barring it altogether from the “core part”. Later, in May 2020, Downing Street adopted a different position, proposing a “5G Club” of 10 democracies (the G7 countries along with Australia, India and South Korea) to create alternative suppliers of 5G equipment and other technologies to avoid relying on China.

The sceptics

The vast majority of Allies have not barred or limited the role of Chinese companies in their 5G infrastructure. In France, for instance, Orange and Vodafone already chose Ericsson (Sweden) and Nokia (Finland) for their 5G networks. Nonetheless, both the government and the intelligence community have signaled that they do not see any valid reason to exclude other foreign providers. Similarly, the Belgian government announced it would impose constraints only on “unreliable suppliers”. Other Allies, such as Canada, have so far taken no decision on Chinese companies.

The early adopter

Finally, another group of countries have already adopted Chinese 5G technology and – given the high replacement costs of the infrastructure – are unlikely to backtrack. Within NATO, these are Hungary and Spain. However, several early adopters, although not NATO countries, are important for the Alliance or some of its Allies. In Europe, these include Ireland, an EU member, and Serbia, a potential future EU member, and Switzerland. Among Gulf States, other examples are Bahrain, Kuwait, Oman, Saudi Arabia and the United Arab Emirates, which to different degrees host military bases or personnel of different NATO Allies. In Asia, Indonesia and the Philippines are among the countries to have adopted Huawei’s 5G technology.

Where next?

The discussion on 5G will continue in the months and years ahead, and the issue is likely to acquire further salience as military communications start to transition to 5G. In the future, for NATO in particular, it will be of central importance to exploit these new technological opportunities for command and control, communications, as well as for other purposes. Without 5G communications, it will be difficult to fully exploit big data, artificial intelligence and cloud computing on the battlefield.

#### 5G cybersecurity is key.

Mark Zeller 22, leader of the Global Sales and Business Development Team for Axellio, 4/20/2022, "Do the risks of the DoD’s shift to 5G outweigh the benefits?," No Publication, <https://www.securityinfowatch.com/government/article/21264867/do-the-risks-of-the-dods-shift-to-5g-outweigh-the-benefits>, RMax

However, the Department of Defense must guarantee that the 5G revolution is as safe as possible. With the confluence of all of these technologies and services, troops and commanders will have access to a vast quantity of data and situational awareness. With so many people relying on a network for critical mission execution, the Department of Defense must ensure that it is safe from start to finish, that it can withstand current cyber-attacks, and that it can self-heal.

The Department of Defense has a long history of fostering innovation by sponsoring innovative technology ventures and pushing the boundaries. With 5G now available and a slew of commercial technologies converging, we'll be able to take advantage of the next big communications revolution while also ensuring its security, resulting in companies clamoring for solutions based on DoD-funded research. Let's simply put security front and center, and make sure it's as high a priority as deployment speed.

#### Integration of 5G into military operations solves everything---BUT fails absent all-of-NATO coordination.

James Jones 20, Executive Chairman Emeritus of the Atlantic Council, former Supreme Allied Commander, former National Security Advisor to the President; Ian Brzezinski, former Deputy Assistant Secretary of Defense for Europe and NATO Policy; Douglas Lute, former U.S. Ambassador to NATO; and Robert Wheeler, former Deputy Chief Information Officer for Networks at the Department of Defense, 8/13/2020, "NATO Must Move Out Smartly on 5G," Defense One, <https://www.defenseone.com/ideas/2020/08/nato-must-move-out-smartly-5g/167687/>, RMax

Much attention is focused, and appropriately so, on the security risks associated with 5G – particularly those technologies produced in China. But next-generation wireless technologies promise a revolution in military operations, one that will change everything from training to logistics to the tactical, operational, and strategic dimensions of warfare. As the institution responsible for enabling effective joint and combined operations by its member states, NATO must help lead the integration of 5G into the force structures and operations of the alliance and among allied armed forces.

Next-gen wireless communications are a game changer because lower network latency and leap in throughput speeds translates into massive real-time data sharing, and because low power consumption will shrink the size and weight of the electronic systems that burden combat aircraft, warships, and individual troops.

5G will bring to the battlefield new ways to share and integrate sensor data between operators, weapons, and platforms, including unmanned systems. It will enable forces to harness artificial intelligence and machine learning in ways never before seen on a battlefield: autonomous loading and off-loading of trucks, trains, planes and ships; enhanced situational awareness for soldiers in the foxhole and their most senior commanders; real-time targeting and retargeting; and, new military concepts of operations, such as the swarming of drones.

Imagine a very high-speed, low-latency secure wireless bubble across a battlefield or all of Europe. Built correctly, this would be the digital backbone of a better NATO defense and deterrence posture.

But along with the opportunities, 5G poses profound challenges for the alliance. If left uncoordinated, allies risk deploying 5G technologies that strip their forces of interoperability and render them vulnerable to penetration and compromise by our adversaries. NATO needs a 5G strategy to mitigate, if not eliminate, those risks and position allied forces on the technological high ground of the battlefields of today and tomorrow.

### Military---Comms--2AC

#### 5G risks compromising military information---mimicking the chain of command wrecks military communications.

Katarina Kertysoba, 02/25/2022; Policy Fellow at the European Leadership Network and a Wilson Center Global Fellow, focusing on conventional arms control, Russia-West relations, Arctic security, and climate-nuclear nexus. Degree in International Relations and French from the University of St. Andrews, and security studies at Sciences Po Paris, and the Moscow State Institute of International Relations; “When 5G meets AI: Next Generation of Communication and Information Sharing” *NATO Strategic Communications Centre of Excellence*https://stratcomcoe.org/publications/when-5g-meets-ai-next-generation-of-communication-and-information-sharing/237//ekc

In the military realm, deepfake technology could disrupt effective military communication by producing false but convincing signal chatter on a massive scale or mimicking key individuals in the chain of command giving voice orders.54 Also consider the implications of high-quality insurgent propaganda video for asymmetric warfare. Creating policies to address this security risk is key for NATO and its allies, as it moves forward in the realm of cyber defense.

Deepfakes make it possible for malign actors to deny the truth in two ways: not only may fake videos be passed off as real to create doubt, but authentic information can be passed off as fake.55 This happened in 2018 in Gabon, when opponents of president Ali Bongo, who had not been seen in public for months, claimed that a video of him produced by the administration was fake, suggesting instead that he was incapacitated or dead. This speculation spread and the military attempted a coup a week later.56

Despite these potential dangers, a recent primer on deepfakes, published by the NATO Strategic Communications Centre of Excellence in Riga, concluded that while the threat from deepfakes is real, it is only one tool among many in the hands of malign actors. The risk posed by deepfakes is narrower than commonly suggested and may distract from other deployments of machine learning by disinformation perpetrators that may be as, if not more, impactful than deepfakes.57

Cyber (in)security

5G is generally considered more secure than previous networks (2G, 3G, 4G LTE) due to better encryption 58 and the ability for network slicing, which makes potential breaches less likely and less damaging.59 Since 5G is an evolution of 4G LTE, developers of this technology have been able to deal with weaknesses and vulnerabilities in previous networks and build security improvements into the protocol to ensure that 5G is more secure. However, that potential for extra security may not be delivered by the service providers for cost reasons. Despite increasing risk, not all manufacturers prioritize cybersecurity. Perhaps the greatest risk concerns extension of the attack surface. As connected devices proliferate in a 5G environment, the threat potential as well as new points of attack increase. Put simply, any system is only as strong as its weakest link: billions of interconnected devices with varied security also mean billions of possible breach points.60 Given 5G’s edge computing potential, this is a concern for the creators of 5G infrastructure and networks across Europe.

Most of the attention surrounding the cybersecurity of 5G networks has focused on supply chain challenges. Chinese companies currently lead in 5G development and Huawei dominates the global market for telecommunications equipment. In 2019, twothirds of 5G networks outside China relied on telecom equipment manufactured in China.61 On top of reported security vulnerabilities – such as software code deficiencies or poor oversight of its supplier networks – which could be exploited by any malign actor, concerns have also been voiced about Huawei’s ties to the Chinese government and the potential risk that China might use 5G infrastructure for espionage or illicit actions (such as intellectual property theft, company sabotage, or fraud).62 The Chinese State Security Law obliges companies to ‘provide assistance with work related to state security’.63 If critical communications, including Internet voting, come to depend on 5G networks, this will create a level of insecurity since the Chinese regime might gain access to and eventually manipulate such processes.64 The ability to manipulate public opinion, with implications for democracy, is certainly there, just like it was with 4G. With 5G, however, the lack of trust in its architecture, alongside uncertainties about how the infrastructure operates, heightens some of those concerns.

In addition to user profiling and political microtargeting, with the roll-out of 5G, an increase in the volume and speed of data theft is expected.65 As confirmed by the US Cybersecurity and Infrastructure Security Agency (CISA), 5G networks will constitute ‘an attractive target for criminals and foreign adversaries to exploit for valuable information and intelligence’.66

### Military---HGVs/NC3---2AC

#### Secure 5G solves HGVs and NC3.

Kevin Zerrusen 19, Senior Advisor to the Chairman for Cybersecurity Policy at the U.S. Securities and Exchange Commission; et al., June 2019, “The National Security Challenges of Fifth Generation (5G) Wireless Communications: Winning The Race To 5G, Securely,” *Intelligence and National Security Alliance Cyber Council*, <https://www.insaonline.org/wp-content/uploads/2019/06/INSA_WP_5G_v5_Pgs.pdf>, RMax

Just as 5G networks’ data capacity will enable a vast array of commercial and civilian applications, so too will it open the door for enhanced military capabilities. As described by the Defense Innovation Board (DIB), a federal advisory committee established to provide independent advice to the Secretary of Defense:

5G has the capability to combine DoD’s current fragmented networks into a single network to promote improved situational awareness and decision-making. This expanded reach will enable new technologies like hypersonic weapons and hypersonic defenses to be deployed, and has the potential to strengthen existing missions like nuclear C3. At an enterprise level, 5G can vastly improve day-to-day tasks such as logistics and maintenance, elevating the efficiency and speed of work across DoD.21

U.S. national security requires that such military communications – as well as communications relating to diplomatic, intelligence, law-enforcement, peacekeeping, and humanitarian activities around the globe, some of them integrated with allies or coalition partners – be secure and reliable. These activities frequently rely on the global ICT infrastructure, as well as the infrastructures of our allies and partners, for all or part of their communications. The potential penetration by China of these infrastructures creates significant risks to U.S. mobilization, sustainment, and mission continuity. The use of Chinese equipment in developing countries’ telecommunications networks will create a global operational environment in which the U.S. forces may be compelled to operate on systems subject to hostile influence or control.22 Even though U.S. forces often deploy with U.S.-origin computing and communications systems that can operate independent of indigenous infrastructure, secure 5G technology can enhance deployed capability.

### Military---Interoperability---2AC

#### NATO is key to winning the tech race – prevents disabling of weapons systems and creates NATO interoperability

Bloch & Goldgeier ’21 [Agneska & James, Agneska Block is a Senior Research Assistant at the Center on the United States and Europe at The Brookings Institution, James Goldgeier is a professor of international relations at the School of International Service at American University in Washington, D.C., October 2021, “FINDING THE RIGHT ROLE FOR NATO IN ADDRESSING CHINA AND CLIMATE CHANGE,” The New Geopolitics: Europe, <https://www.brookings.edu/wp-content/uploads/2021/10/FP_20211026_nato_china_climate_bloch_goldgeier.pdf>, St. Mark’s, AM]

China’s challenge to NATO as a military alliance arises not only from its deployments, but its technology investments, including in 5G, as well as its role in supply chains, which could disrupt NATO military interoperability or create a Chinese capacity to disable weapons systems.16 As Julie Smith, Andrea Kendall-Taylor, Carisa Nietsche, and Ellison Laskowski have argued, “NATO interoperability requires member states to have secure and resilient telecommunications infrastructure, which Chinese systems put at risk. Moreover, if the allies diverged in their responses to the China challenge, the result could be the adoption of different standards, which would also undermine the interoperability of forces.”17 In response, NATO member states should be able to count spending on secure 5G systems toward their 2% of GDP defense spending target.18 While the United States is restricting Chinese telecommunications giant Huawei from access to its 5G networks, the range of reactions across the alliance is varied.19 Berlin is continuing to employ Huawei access, and although Paris favors Swedish and Finnish providers, it has not formally excluded the Chinese company.20 Ottawa, the lone holdout of the Five Eyes on banning Huawei from its networks, has yet to reach a verdict as of mid-October 2021,21 while Warsaw is pursuing Huawei’s removal from Polish 5G networks.22

### Military---Air Power---2AC

#### Network vulnerability compromises airpower.

Valerie Insinna 22, Senior Reporter covering Air Warfare at Breaking Defense, 1/19/2022, "As 5G rollout begins, Pentagon still doesn’t understand impact on military aircraft," Breaking Defense, https://breakingdefense.com/2022/01/as-5g-rollout-begins-pentagon-still-doesnt-understand-impact-on-military-aircraft/, RMax

WASHINGTON: Today, after multiple delays and months of negotiations with the airline industry, Verizon and AT&T will begin rolling out 5G nationwide, in a move the commercial aviation community says will have dire safety implications.

Airline executives warned in a Jan. 18 letter that, without safeguards in place around airports and runways, the rollout could cause “catastrophic disruption” and “economic calamity.” Despite an agreement by Verizon and AT&T on late Tuesday to limit 5G services around major airports to prevent interference, some international airlines such as Emirates and Lufthansa canceled flights to the United States due to concerns about potential effects on the Boeing 777.

But for a controversy that’s dominated headlines and reached the desk of the president, the Pentagon — the largest aircraft fleet owner in the world — has remained largely silent. That’s because right now, it doesn’t know how 5G will affect military aircraft.

All told, it will be at least a year and a half after the Federal Communications Commission began selling spectrum for 5G before the Defense Department weighs in on the issue, and it could take months after that for the department to come up with a plan to resolve any technical failures that occur as military pilots continue flying in areas where the 5G deployment is occurring.

The overarching problem shared by both the military and civil aviation revolves around radar altimeters, a piece of hardware used by airplanes, rotorcraft and even some drones to measure the height of an aircraft from the ground.

In the United States, 5G will reside on a neighboring portion of the C-band spectrum to radar altimeters. Some aviation experts and government officials are concerned that the resulting interference could prevent aircraft from being able to make landings in bad weather — or worse, that pilots may not truly understand an aircraft’s distance from the ground, increasing the risk of a crash.

“The DoD continues to work very closely with our FAA counterparts on this issue. All DoD Services issued bulletins to the field/fleet, making aircrews aware of the potential for interference and establishing a mechanism to report instances of interference,” said Lt. Col. Dylan McDermott, the Pentagon’s point person on this issue in his role as head of the Aviation Cyber Initiative, co-chaired with the FAA and Department of Homeland Security.

While military pilots will be advised of the potential issue, the department has not issued any NOTAMS — a “notice to air missions” that spells out hazards and or other abnormalities in the air — for any of the military bases in 5G deployment areas, McDermott said in a Jan. 18 statement to Breaking Defense.

#### DoD is not aware of 5G security threats to airpower in the status quo.

Stephen Losey 22, air warfare reporter at Defense News, 1/19/2022, "Military may take months to gauge 5G safety risks to aircraft," Defense News, https://www.defensenews.com/air/2022/01/19/military-may-take-months-to-gauge-5g-safety-risks-to-aircraft/, RMax

WASHINGTON — As the commercial airline and telecommunications industries scramble to limit the potential safety risks to aircraft from a rollout of new 5G networks, it may be months before the U.S. military has a handle on whether, or how big, of a problem this might be for its own planes.

At the center of the controversy is whether the deployment of 5G networks, operating along a frequency known as the C-band, will interfere with radar altimeters used by military, civilian and commercial aircraft and helicopters. These altimeters are used to measure the distance between the aircraft and the ground.

For the military, they are particularly necessary when mobility aircraft such as cargo planes or tankers land in adverse weather conditions. If the pilot’s visibility is poor during such a landing, he or she would have to use altimeters to measure how far off the ground the aircraft is during the approach, and a flawed reading could lead to a crash.

Verizon and AT&T began activating their 5G networks on Wednesday, promising much faster wireless service speeds than the previous 4G network. But amid a growing outcry from the commercial airline industry, the companies on Tuesday announced they would temporarily limit the deployment of new 5G networks near some airports. Some international airlines announced plans to cancel certain flights to the United States over the concern.

### Military---Readiness---2AC

#### 5G insecurity collapses readiness.

Veeli Oeselg 22, Partner at CIVITTA, M.Sc. in Business Administration from the University of Tartu; et al., June 2022, "Military Movement: Risks from 5G Networks," <https://ccdcoe.org/uploads/2022/06/Report_Military-Movement-Risks-from-5G-Networks.pdf>, RMax

5. Military Movement Related Cybersecurity Risks and Mitigation

5.1 Risks Associated with Military Movement Scenarios

In this section of the report, the aim is to give a systematic and high-level security analysis of the use cases given in the previous sections. Threat modelling approaches suit this purpose as they are utilised for comprehending possible threats at the initial stages of development life cycles, even though they can also be helpful in later phases or hypothetical use cases. More specifically, the STRIDE (a mnemonic for Spoofing, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privilege) approach applied to many software developments projects 44 and adopted into complex cyber-physical systems in numerous studies is used. 45 The risks listed below were identified by this method, however, the specific approach is not described to ensure the simplicity of the document.

Both seaports and road transportation solutions are part of the critical infrastructure for logistics and need to have high demands on data security for functional safety and reliable connectivity. The exchanged data and information can be considered as sensitive assets that need to be protected from cyberattacks and enemy exploitation. Both the smart seaport and smart road transportation assets with a risk exposure to cyberattacks include:

* information assets: data in transit, user data, control signalling, network management data, and data stored in data centres;
* infrastructure assets: systems, hardware, platforms, and applications.
* Threat actors include organised cybercriminals, nation states, hacktivists, terrorists, and insiders. These attackers are generally motivated by three main factors: money by ransom blackmail, stealing of business sensitive information and data, and finally sabotage. Exploited security weaknesses are:
* improperly designed IT security policy that is also not enforced, monitored or constantly tested;
* lack of hardening and insecure configuration of the network;
* operational procedures;
* lack of visibility, control, and monitoring.

Figure 9 shows the attack surfaces on network infrastructure that can be exploited by a cyberattacker. Cyberattacks can have severe implications on smart transportation infrastructure and use cases with high cost for protection and mitigation, and unknown losses due to stolen property (data) and losses in productivity. The impacts of cyberattacks in severe conditions could be devastating for logistics and transport solutions vital for the military movement.

[Figure 9 omitted]

In addition to general 5G network-related risks, there exist a multitude of different types of risks related to 5G Core, RAN, cloud services and even from an operational security perspective, as shown in Figure 10. For example, attacks against 5G RAN via jamming operational systems could cause convoys and port machinery to halt operations and cause system shutdowns; and malicious interception can reveal information about military unit locations, their composition, and route. It is therefore important to stress the fact that UE networking and MEC related threats, that are the key element of this research report, are not the only risks and threats but are analysed to the extent of the report’s scope as the military transportation related use cases will be based on multi-access edge computing.

[Figure 10 omitted]

5.2 Multi-Access Edge Computing Related Cybersecurity Risks

According to the network architecture and the use case specificity, both the smart seaport and smart road transportation use cases will rely on multiaccess edge computing technology due to the demand for reliable low-latency data exchange and extensive processing. For smart road transportation, there is evident need for ProSe device-to-device communication relying on a PC5 link channel. When relying on MEC technology, a variety of risks in addition to generic 5G network-related risks need to be taken into account to ensure a high level of security. As for the MEC technology, the computational part, i.e. real-time safety camera stream processing, will move closer to the user and occur at the edge of the network, and third-party attacks and threats can be directly linked to the vehicles and equipment that are used for the transportation of military assets. Therefore, at every stage of the value chain, certain types of risks that can harm both the systems, monitor the movement, or even damage the assets, need to be evaluated. Below is a list of detailed vulnerabilities relevant to MEC. 46

* Improper mechanisms for monitoring, collecting, and storing secure data and transmitting data between devices, which lead to unauthorised access to data and potential fraud committed by the attackers.
* Improper access control to information, where the MEC platform should only provide the mobile edge application with authorised information. If the platform is not secured properly, unauthorised parties can access secure data and confidential information.
* Lack of or improperly implemented DDoS protection. Due to the distributed nature of edge computing deployments, appropriate DdoS mechanisms may be impractical to deploy. Alternative protection mechanisms, therefore, need to be implemented to deter attacks. In the case of a DdoS attack, the attacker can shut down the whole system and halt or alter the convoys transporting the military assets.
* Improper isolation of resources whereby both physical and logical resources should not be shared with other parties/components which have different level of criticality. This means there should be a different level of criticality and security for military-related activities in transportation cases, otherwise there is a high risk of unauthorised access, interception, and eavesdropping by attackers.
* Improper physical and environmental security of edge computing facilities. Edge computing facilities are, by their nature, seated in locations distributed geographically. Normally, the first choice will be communications shelters already operated by the MNO. While communications shelters have physical security controls in place, these are calibrated to risks associated with the communication equipment. Improper security can lead to the destruction of edge computing facilities, causing the connection to shut down and may lead to unlawful interception or loss of data.
* Vulnerabilities in MEC applications that may be used as an entry point for attacks aiming to exploit the virtualisation environments, provide unauthorised access to data, elevate privileges or bring about denial of service, potentially halting equipment loading in ports or halting the platooning convoys on roads.
* Use of a system function without successful authentication based on the user identity and at least one authentication attribute (e.g. password, certificate) opens up opportunities for exploitation and limits accountability, which can lead to information leakage to the attacker regarding the equipment being transported or the location and route of the convoys.
* Security log troubleshooting failure where compromised VNFs are used to generate a massive amount of logged data on the hypervisor, overriding the initial and relevant log entries and making the analysis of logged data futile.
* Software vulnerabilities: Execution of code that exploits existing vulnerabilities on running software and flaws within the MEC system such as buffer overflow. Data overflow can cause unpredictable changes in the system that can potentially halt the military use cases, causing shutdowns in ports and in convoys.
* Data exfiltration/destruction where the data from a compromised entity is transferred or destroyed without the required authorisation, affecting the system backend and necessary documentation.
* Malicious code injection where a malicious piece of code is injected into an active service by the attacker, or an executable file being transferred causing a loss of system integrity, availability, and confidentiality of data.

All relevant stakeholders, including NATO and the military, need to take into account the multiple risks that arise with MEC technology. As this report demonstrates, NATO countries need to deal with continuous risk assessment about vulnerabilities, threats, and the high risks associated with untrusted 5G vendors, technology, and infrastructure. Improper system design and lack of continuous risk monitoring leaves an open gap for potential attackers to penetrate systems and get access to high-confidentiality military data and potentially damage military assets when equipment is being unloaded in ports or transported via road.

The following chapter proposes multiple mitigation measures for cybersecurity related risks, which if followed, can significantly decrease the potential of malignant attacks on military infrastructure and assets.

### Military---Tech Leadership---2AC

#### Leading in the military 5G race underpins all of the tech race.

Erica Borghard 19, Assistant Professor at the Army Cyber Institute at West Pont; Shawn Longernan, Research Scholar at the Army Cyber Institute and U.S. Army Reserve officer at the 75th Innovation Command, 4/25/2019, "The Overlooked Military Implications of the 5G Debate," <https://www.cfr.org/blog/overlooked-military-implications-5g-debate>, RMax

Last week, the U.S. Defense Innovation Board released a report outlining the risks and opportunities for the United States in the global race to develop 5G. This followed a damning report published by the United Kingdom’s Huawei Cyber Security Centre Oversight Board detailing how the Chinese telecom giant’s 5G products, particularly its software, contained significant vulnerabilities and that the company had failed to remedy persistent poor security practices. 5G network architecture uses high frequency spectrum to enable significantly faster speeds to process larger amounts of data with lower latency and greater device connectivity. While much attention has been paid to economic and espionage implications of a potential Chinese lead in developing and operating 5G infrastructure, there are important military implications that remain largely overlooked.

There are economic implications for which entities can secure the greatest global market share of 5G technology. Technological innovation drives economic growth, job creation, and global economic influence. Huawei may have a long-term market advantage over U.S and Western telecoms because the former has been able to offer 5G products at far cheaper rates than the latter. Furthermore, there are also concerns that Chinese-built 5G technology is likely to contain backdoors that could be used to enable Chinese economic or national security espionage. It is unlikely that Beijing would actively monitor all of the content of the data that comes across Huawei owned or operated infrastructure (although it may collect and analyze metadata). However, it is conceivable that Huawei would get a proverbial “tap on the shoulder” from Beijing to share pertinent information in specific instances. This may include individually targeting senior corporate executives, which is enabled by the millimeter wave frequency that 5G networks employ.

The military applications of 5G technology have vital strategic and battlefield implications for the U.S. Historically, the U.S. military has reaped enormous advantages from employing cutting edge technology on the battlefield. 5G technology holds similar innovative potential. Perhaps most obviously, the next generation of telecommunications infrastructure will have a direct impact on improving military communications. However, it will also produce cascading effects on the development of other kinds of military technologies, such as robotics and artificial intelligence. For instance, artificial intelligence and machine learning capabilities, such as those used in the Department of Defense’s Project Maven, could be greatly enhanced when leveraging the data processing speeds made possible through 5G infrastructure. As an era of great power competition emerges between the United States and China, the United States has a compelling strategic interest in being at the forefront of these new technologies.

The United States and its allies must also consider the tactical and operational implications on the battlefield of conducting conventional or counterinsurgency operations in an area with Chinese owned or operated 5G infrastructure. This concern stems from the nature of the relationship between Huawei, an ostensibly private company, and the Chinese Communist Party (CCP). While Huawei’s founder and CEO, Ren Zhengfei proclaimed in a February 2019 interview on CBS This Morning that the company never has and never would provide information to the Chinese government, many experts are skeptical. Under China’s 2017 National Intelligence Law, the CCP has the authority to monitor and investigate domestic and international companies as well as direct organizations to assist with government espionage efforts. As such, it is conceivable that Huawei will be required to hand over its data to the Chinese government for collection and analysis.

Due to this reality, the United States must consider and be prepared to conduct overseas contingency or counterterrorism operations in areas where Chinese telecommunications infrastructure is widely proliferated, thus restricting the United States’ ability to rely on indigenous telecoms. As noted by US AFRICOM Commander General Thomas Waldhauser, this has already become an issue in Africa where Chinese telecommunications companies are poised to dominate. The integrity of U.S. military communications systems that rely on 5G networks could be undermined at key phases of an operation. For example, if the United States is conducting a military operation in an area of interest to China, it is plausible that the Chinese government could leverage Huawei to intercept or even deny military communications. Furthermore, Chinese telecom infrastructure dominance in a theater of operations may limit the U.S. military’s ability to conduct precision targeting that leverages signals intelligence collection on 5G telecommunications networks.

The strategic and battlefield implications of who owns and operates 5G infrastructure around the world underscores the national security importance of 5G. The U.S. government and its allies should more systematically assess both the opportunities and risks associated with conducting future military operations in environments that rely on Chinese technology.

## Answers

### Military---AT: 5G Not Key---2AC

#### Only 5G solves future NATO military requirements---nothing else satisfies latency and range requirements for communications, flexibility, and security.

Capela ’21 [Germano; July 2021; Radio Engineer at the NATO Communications and Information Agency, M.S. in Electrical and Computer Engineering from the Instituto Superior Técnico, M.Sc. in Electrical, Electronics, and Communications Engineering from Escola Naval; et al.; "5G for deployable and maritime communications," https://doi.org/10.1109/ICMCIS52405.2021.9486397]

In [1], the authors have noted the potential of 5G technologies for military applications and their significant interest for specific areas, namely Deployable Communications and Information Systems (DCIS) and Maritime Coastal Communications. In this context, NATO Allied Command Transformation (ACT) tasked the NATO Communications and Information (NCI) Agency to pursue capability development applications of 5G technology in specific scenarios that could bring benefits to NATO.

Effective and reliable command and control (C2) of military operations, particularly those involving any form of mobility, require the use of radio communication networks. In military scenarios, the utilization of radio networks usually entails deploying infrastructure in remote areas and in highly mobile military assets, where other traditional means of communication are not available or are not stable and reliable enough to cope with mission requirements.

The DCIS domain covers a wide range of expeditionary coalition operations, which may occur anywhere in NATO’s or national areas of interest. In this paper, we address NATO provided infrastructure, but the same concepts also apply to national implementations. DCIS systems are self-contained, transportable infrastructures and they have the challenges of providing information services and interconnecting remote headquarter locations (HQs), while being easily assembled and torn down by common uniform personnel.

C2 in maritime operations is a complex construct by itself due to the intrinsic mobility of naval platforms. Owing to the complexity of military vessels and wide range of areas of operation – inshore, shallow and blue waters – the range of suitable communication systems for maritime operations is very limited and consists of either expensive satellite reach-back links or limited capacity, long haul high-frequency (HF) connections.

The use of highly deployable, easy to install and operate radio systems in military scenarios has been addressed in the literature and has followed the natural evolution of wireless technologies. With the advent of Worldwide Interoperability for Microwave Access (WiMAX), which is a QoS-oriented radio access technology, [2] and [3] investigated its adequacy for mission-critical communications in the subject scenarios, but the shortfalls outnumbered the eventual advantages of fielding WiMAX in military contexts. More recently, the use of Long-Term Evolution (LTE) and other International Mobile Telecommunications (IMT) technologies has also gained interest for military applications and it was thoroughly investigated in [4]. However, there is broad consensus that complexity of deployment, lack of proper spectrum supportability, limited throughput and overall security measures do not meet military requirements.

In this paper, we propose novel contributions to the military communications scientific community by developing a proof-of-concept experiments for two priority scenarios – Small Operational Deployable HQ (from the Deployable CIS domain) and Coastal Communications (from the Maritime Communications domain) – for assessing the adequacy and maturity of existing and available 5G technologies for military applications. 5G technologies represent a paradigm shift in IMT standards and have tremendous potential for military applications, as discussed in [1]. Fig. 1 depicts the envisaged proof of concept scenario, where both maritime and deployable domains are combined in the same testing setup and geographical area.

This paper focuses on the 3rd Generation Partnership Project (3GPP) [5] Release 16, as the target for existing and available features, while Release 17 and beyond is regarded as soon to be available features. The paper discusses the specific challenges and defines concepts, architectures and metrics to be validated under experimental conditions, with specific requirement and test parameters, and with further intention to conduct and report on the experiments. To our knowledge, this approach has not been presented in the literature and it is deemed fundamental for informed scientific discussions on the subject.

Section II describes and explores the potential 5G enablers for military applications and clarifies the importance of experimentation and validation activities. Sections III and IV outline the requirements for two proof-of-concept experiments, first for a Deployable CIS scenario and then for a Maritime Communications scenario. Finally, section V concludes and discusses the expected outcomes for the experimental endeavour.

SECTION II.

5G For Military Applications

On the technical side, NCI Agency conducted an assessment of 5G technologies and their potential for military applications in a number of reference scenarios. This work is reported in a technical working paper [1], which gathered broad interest and support from Allies, partners and military stakeholders. Owing to the complexity of the topic and to the evolving nature of 5G specifications, the proposed effort contributes to: a) Assessing technology readiness of 5G technologies, with a scientific methodology; b) Identifying opportunities and gaps in 5G technologies for military application; c) Further develop priority 5G military scenarios and concepts; and d) Providing conclusions and recommendations for follow-on discussions with stakeholders. This paper investigates a Small Operational Deployable HQ and a Coastal Communications scenario – representing the Deployable CIS and Maritime Communications domains respectively – which were identified in [4] as high value and relatively low complexity to realize in the short term.

Military operations are prone to unforeseen events and changing operating conditions but on the other hand, the actual level of skilled support, on the field, to address highly complex technical challenges, is limited. Hence, any deployed communications system – regardless of the domain – needs to be flexible and simple enough to be operated by unskilled personnel and to be easily installed/torn down. Complex electromagnetic (EM) environments and scarce spectrum resources also limit the range of viable radio-based communication solutions. Hence, the coexistence among other radio systems has to be accounted for and such systems must be able to adapt to new operating conditions. Moreover, hostile EM environments also impose constraints to the use of radio-based communication systems. This is highly dependent on the nature of the operation and not a constant variable along its existence.

The dynamism of available spectrum resources and intrinsic mobility of forces poses significant challenges to any type of military communications. 5G New Radio (NR) features, such as multiple-input multiple-output (MIMO), beam forming and comprehensive spectrum support – Frequency Range (FR) 1 (410 to 7,125 MHz [6]) and FR2 (24.25 to 52.60 GHz [7]) (as of Release 16 [8]) – covers a wide range of communication scenarios and offers numerous possibilities for agile and harmonized radio systems. While FR1 provides coverage-capacity tradeoffs, FR2 enables high bandwidth (but lower range) use cases. The advent of NR–U, as a flexible way to use and combine unlicensed and licensed spectrum [9] is also an enabler for improved spectrum agility. When compared to other commercial systems, 5G NR enables numerous options and intrinsic agility, which is deemed extremely relevant for military scenarios.

Another key feature of military scenarios is the ability to operate without resorting to fixed infrastructure. In that regard, the work developed by 3GPP to introduce Integrated Access and Backhaul (IAB) [10], mobile edge computing [11] and to improve Sidelink [12] is an indicator that 5G has enough features to support on-the-move and infrastructureless networking. Major IAB features and Sidelink improvements are introduced in Release 16 and subsequent improvements considered for Release 17. Nevertheless, these technologies are still immature and do not have relevant market adoption yet. In fact, other industry verticals, such as critical communications and automotive sectors, have the exact same need as military users, which is to be able operate in an infrastructure-less fashion. From a military standpoint, the lower the chain of command, the more important mobility and resilience enabling features are.

The military also extensively relies on various satellite networks to cope with deployability and mobility requirements and their use is of particular interest to land expeditionary and maritime operations. In Release 16, 3GPP introduced the concept and started studying non-terrestrial networking (NTN) [13] based on 5G NR, which consists of using airborne or spaceborne vehicles as part of a 5G NR-enabled radio access network. NTNs have the potential to increase the coverage in deployed and tactical use cases by allowing users to seamlessly roam between terrestrial and non-terrestrial networks, i.e. to provide service continuity between two different radio access networks without any service interruption. Even though NR over NTN specifications are expected for Release 17, it is important to regard NTN’s potential in light of potential use of 5G for military applications.

It is anticipated that the use of 5G in military scenarios comes with several practical and technological challenges, particularly regarding the context of use of commercial technologies:

Carrier-grade radio technologies typically require a comprehensive deployment planning, they require highly skilled personnel to be operated and maintained and their assigned spectrum resources are typically stable and well defined. This could be limiting for high-tempo deployments and operations.

Commercial technologies are not tailored to operate through challenging and non-benign EM environments, which comprise compatibility with other friendly radio systems and coping with intentional interference (i.e. radio jamming). Deployment complexity and threat level can limit the use of commercial technologies.

As a result of the investigations in [1], in the next chapter the authors propose two proof–of–concept propositions for near-term experimentation of expeditionary and maritime scenarios and concepts.

SECTION III.

Small Operational Deployable Headquarters

A. Introduction

In this section, we propose an experiment, using the combined 5G proof-of-concept prototype, to assess the feasibility of 5G-enabled concepts for providing combined wireless metropolitan area network (WMAN) and wireless local area network (WLAN) distribution in support of small operational deployable headquarters (DHQ) for NATO and national expeditionary operations. Small Operational DHQ scenarios regard expeditionary operations and the operational level of command (for command & control (C2)), and consider the use of high-performance 5G systems to provide wireless connectivity inside the DHQ (right portion of Fig. 1), as enabler of quick DHQ setup and teardown.

B. Technical Concept

Small DHQs are made up of a few tents and shelters scattered around a limited fenced-off area, typically resulting in a geographical footprint of less than 0.25 km2, with maximum ~300–m distances between the central CIS location and remote locations. Although these headquarters are at the operational level of command, they are expected to be deployed relatively closer to subordinate tactical headquarters and are also expected to be subject to limited, but unneglectable, electronic warfare (EW) threats, at least during the initial stages of the operation.

When threat levels are deemed low (i.e., when it is possible to deploy wireless systems), one could consider using combined WMAN & WLAN distribution from a single wireless point-to-multipoint (PTMP) system wirelessly connecting a central CIS location to network terminals (phones, computers and other devices), to enable very short DHQ establishment times (in terms of CIS connectivity), without the need to lay local area network (LAN) cables between tents (using tactical fibre optical cables) and then to network terminals (using cabled LAN infrastructure).

Currently, NATO does not use these concepts for two reasons: commercial technologies, such as Wi-Fi systems, do not offer suitable performance to be used as a combined LAN access and LAN distribution systems in small DHQs, and traditional IMT technologies, such as LTE, have limited system capacity and are not available in frequency bands of interest for military applications. When compared to carrier-based solutions, Wi–Fi tends to fall behind in terms of range, spectrum agility, mobility management and overall QoS. Hence, a 5G solution would provide superior coverage, requiring less infrastructure density/complexity, while assuring superior QoS features. Moreover, 5G NR enables the combined use of licensed and unlicensed bands, which is of great advantage in this scenario. Through 5G NR-U (NR for unlicensed bands), one can provide nominal capacity by anchoring the system in a military band (e.g. 4.4 - 5.0 GHz), while using the 5 GHz industrial, scientific and medical (ISM) band as supplementary band, when and where available for use. This way, a high degree of service quality is provided, since the system can assure ‘a minimum and guaranteed’ capacity through a licenced band, and increase its capacity by aggregating available unlicensed bands.

Current solutions in NATO DCIS resort to wired LAN distribution systems for practical reasons – to provide adequate capacity and to cope with existing security policies (which prevent using wireless LAN systems for higher classification domains).

Deploying a combined wireless LAN distribution and access system based on 5G technology (which has intrinsic advanced mobility management features) would provide significant operational benefits, such as:

* Fast DHQ setup and tear-down times.
* End-to-end quality of service (provided that encrypted traffic is appropriately recognized by the system).
* High mobility for C2 personnel to roam inside the DHQ.

C. Requirements for a 5G-based Proof of Concept

Due to the nature of small DHQs, the proposed architecture is predicated in privately owned and operated infrastructure, which represents the most flexible and agile type of employment such a concept could be used, i.e. out of area operations where public infrastructure is not available/does not exist.

For this architecture, illustrated in Fig. 2, a single-tier high-capacity 5G-based combined WMAN/WLAN system in the 5G Sub-6-GHz (mid) frequency band, ideally in the 4.4-5.0 GHz band (often referred to as NATO Band IV), would provide both capacity and flexibility: a single 5G base station (gNB) would provide both high capacity (i.e., up to a total system capacity of up to ~4 Gbit/s over a 400 MHz wideband radio channel) and mobility around the small DHQ, as the tents are mostly transparent to radio frequencies. Users could use this infrastructure to carry all application services (real-time and non-real-time traffic, etc.).

Using the 4.4-5.0 GHz band, while not ideal for mobile communications but desirable for spectrum management aspects, would be compensated by the high-performance features of 5G NR, such as beam forming and massive MIMO, as well as the fact that tactical tents are electromagnetically transparent (as opposed to buildings). While the WMAN/WLAN system can rely on the 4.4-5.0 GHz band to provide the regular capacity, additional portions of unlicensed spectrum (5 GHz band) can supplement capacity in surge moments or whenever available. This can be achieved through 5G NR–U, where the 4.4-5.0 GHz band would become the anchor band and the 5 GHz the supplementary band.

### Military---AT: HGVs Bad---2AC

#### Hypersonic missiles are inevitable because of R&D increases---ensuring low latency via 5G ensures they are effective and successfully countered.

Michael Zurat 22, Senior Solution Architect at General Dynamics Information Technology, 3/7/2022, "Why 5G Is a Top DoD Priority," <https://www.gdit.com/perspectives/latest/why-5g-is-a-top-dod-priority/>, RMax

As a DoD example, current radios provide limited support for controlling devices traveling at hypersonic speed. The U.S. doesn’t have operational hypersonic missiles yet, but it’s a top priority. According to the Government Accountability Office, funding for hypersonic research increased by 740% between 2015 and 2020. The 2022 defense budget alone increased funding by 20%.

Managing and intercepting hypersonic devices will require the ultra-low latency 5G provides. This is a must have for manned and unmanned teaming (MUMT), which pairs manned and unmanned autonomous devices for enhanced mission delivery. Connecting operators, drones, and other vehicles all with 5G’s high-band, near-zero latency capability, along with operating on and through existing commercial networks in partner nations, would be a competitive advantage against peer and near peer adversaries. It would also form the underlying infrastructure for enabling JADC2 and coordinating with NATO and partner nations.

#### 5G is key to preventing HGV instability.

John Grady 20, 6/30/2020, "Officials: U.S. Must Move Faster in Testing and Fielding Hypersonics, 5G Networks," <https://news.usni.org/2020/06/30/officials-u-s-must-move-faster-in-testing-and-fielding-hypersonics-5g-networks>, RMax

The best way to counter China’s and Russia’s high-tech advances is to change the Pentagon’s and Congress’ risk-aversion culture and embrace quicker – but still robust – testing and fielding of programs, a senior defense official said Tuesday.

Mark Lewis, [speaking at an online forum of the Hudson Institute](https://www.hudson.org/events/1835-video-event-a-conversation-with-dr-mark-lewis-on-the-pentagon-s-defense-modernization-priorities62020), said, “there are dumb failures and noble failures” in testing. Some of the “dumb failures” occur because the testing was not rapid or robust, which has the potential to sink a project but is also easily fixable in the future.

In looking to avoid that mistake, the director of defense research and engineering for modernization added, “we recognize we are in a race,” particularly with China in the development of hypersonic weapons and the application of 5G connectivity to the battlefield.

All too often, there has been a failure to transition from science, technology, research and development projects to full production because they lacked continuous testing or there was an unwillingness to accept any failure, he said.

Speaking at the Atlantic Council in another online security forum on modernization, Michele Flournoy, former undersecretary of defense for policy, called that gap “the graveyard” of promising technology that needs to be eliminated.

“We have to get Congress to trust DoD taking more risk” in testing new systems like hypersonics, she added.

Lewis also used hypersonics as an example, saying “we really do think it’s a game-changer” in military thinking. These systems offer speed, maneuverability and trajectory and range.

Because they are in the atmosphere but moving at five times the speed of sound, hypersonics weapons “are more difficult to detect from the ground and from space.”

Right now, the [Pentagon is looking at “a high-low mix” of hypersonics](https://news.usni.org/2020/06/22/house-defense-bill-pushes-hypersonic-weapons-for-zumwalt-destroyers-slows-lusv-procurement), as it did with the F-16s and F-22 fighters to balance capability and cost. That means testing and eventually fielding boost-glide and air-breathing systems.

He predicted initial deliveries by the mid-2020s, with 40 flight tests for both systems before then.

“Our competitors should not doubt that we are … in a very aggressive program” of testing and development, Lewis said.

[At the Atlantic Council](https://www.atlanticcouncil.org/event/the-future-of-high-tech-warfare/), retired Marine Corps Gen. James Cartwright said developing “technology is the easy side of the question. What do we want to do with our security as we go forward” was the unanswered question. Flournoy said some answers could come through more wargaming on innovative concepts of operations on new systems like hypersonics and advanced technologies like 5G.

Using the connectivity of advanced telecommunications as an example of what future needs will be, Lewis said, “we don’t see 5G as a single goal post.” He termed it a technology that will change over time. “It allows us to do many more things” than were possible in earlier technologies and provides resilience not available in the past. The 5G advantage now is it “provides full connectivity of services and sensors — the internet of things” and allows the services to operate in any environment or domain.

He added, “China is making a big play on the hardware side” of 5G. But potentially more troubling is China’s [attempt to set standards on use and operations, particularly through Huawei](https://news.usni.org/2020/04/09/veneer-of-chinas-charm-offensive-cracked-by-vietnamese-fishing-boat-incident), an international telecommunications and information provider corporation.

Like it did with 4G, “we think the United States has to lead and set the standards … for deciding the future,” Lewis said. The United States has consistently warned allies and partners the danger that Huawei poses to their security by installing backdoor software to spy on or alter critical infrastructure. U.S. protests have met only with middling success, even in Europe.

Christian Brose, author of Kill Chain and a former staff member of the Senate Armed Services Committee, said at the Atlantic Council forum that the Chinese Communist Party has been “systematically building a military to counter the United States” using advanced technologies.

Lewis said they “learned from us” as the United States rested on its laurels of stealth, making early investment in hypersonics and artificial intelligence and continuing to invest in these areas.

Cartwright drove home that the technologies aren’t just there for technology’s sake, but rather have operational implications if a conflict arose.

“The systems are there [inside the Pentagon]; the cultures are not” to “go very, very fast” in applying software that aid decision-making and response in a crisis, Cartwright said. Instead of thinking days or weeks are available to move forces, the response needs to be available “at the speed of gaming” through artificial intelligence and 5G.

#### 5G ensures effective defense.

Jamie Carter 19, technology journalist for Techradar, 6/13/2019, "How the 5G network could benefit the military," TechRadar, https://www.techradar.com/news/how-the-5g-network-could-benefit-the-military, RMax

5G and hypersonic weapons

With a super-fast network able to exchange data in real-time over vast areas, 5G could have a role to play in something that’s long been talked about in the military: hypersonic weapons.

Now being developed by Russia, China, the USA and France, seemingly for 2022, hypersonic weapons will travel at Mach 5 – five times the speed of sound – and will cover a mile per second.

They will also fly at very high altitudes and on unpredictable flight paths, easily skirting existing missile defense systems. Intercepting them is therefore very difficult, but so is guiding them.

Where 5G comes in, is in hypersonic defense systems. An aircraft carrier, a military base, or even a city, is going to have less than a minute to react to an incoming hypersonic missile.

In short, incredible amounts of artificial intelligence-powered real-time data processing on targets and trajectories are going to be required to stand any chance of defending against hypersonic weapons. Cue 5G.

### Military---AT: HGV D---2AC

#### HGV defense doesn’t assume accidental launch and nuclear first strikes caused by perception risks.

Jeffrey Hill 19, Mobilization Assistant to the Commander of the Sixteenth Air Force, Major in the U.S. Air Force, 2019, “Hypersonic Highly-Maneuverable Weapons and Their Effect on the Deterrence Status Quo,” *Assessing the Influence of Hypersonic Weapons on* Deterrence, Chapter 4, <https://media.defense.gov/2019/Sep/25/2002187108/-1/-1/0/59HYPERSONICWEAPONS.PDF>, RMax, HS/HM = hypersonic and highly-maneuverable

Are HS/HM Weapons Destabilizing?

It has been demonstrated that none of the great nuclear powers require HS/HM weapons to achieve a credible retaliatory strike capability. The volume of both Russian and Chinese current land-based ballistic missile arsenals taken individually make each countries’ second-strike capability unquestionable. There is no established need for either country to develop HS/HM weapons as a means to assure this capability. Using current capabilities and fielded forces, the United States, Russia and China all maintain robust nuclear deterrence forces that maintain the established status quo that has prevented great-power conflict for seven decades. From a strictly technological aspect, HS/HM weapons have not altered each countries’ ability to achieve a credible retaliatory capability and as a result have not fundamentally changed the deterrence status quo from this perspective. However, as HS/HM weapons create new capabilities and alter how decisions are made and how long a country has to make a retaliatory decision, these weapons are seen as more threatening and aggressive than current fielded forces. This perception has the potential to destabilize the status quo.

As these weapons are significantly harder to track and terminate than traditional ballistic warheads and as they create a shortened timeline to make a retaliatory decision prior to receiving a potential first strike, they are seen as naturally offensive weapons that are far more threatening and aggressive. As described earlier, a country at risk of receiving an HS/HM attack has a significantly reduced timeline (from the point of detecting an incoming HS/HM weapon and warning) to make a decision as to a retaliatory strike prior to receiving the first hit. Complicating matters further, the aggrieved country has little capability to determine the most likely impact point of such a strike meaning any retaliatory efforts are not likely to be calculated to achieve a proportionate response making any retaliation naturally disproportionate. These issues complicate the decisionmaking process for a threatened country, which will likely drive changes to that country’s deterrence posture.

The most concerning aspect of this new calculus is the possibility of a country that is threatened by HS/HM strikes to adopt a “launch-on-warning posture” or a possibility of moving towards a policy of preemptive strike.61 A launch-on-warning posture relies heavily on a very robust and highly accurate warning apparatus that is not prone to misidentification of threats, which is dubious at best and a preemptive strike posture would fundamentally change the longstanding deterrence postures of the great nuclear powers. Both possibilities would lower the threshold for use of nuclear weapons in warfare and, especially in the case of a launch-on-warning posture, significantly increase the probability of accidental launch.

Of further concern is the threat that HS/HM weapons represent to no-first-use policies established by all three great nuclear powers. It is currently challenging to launch a preemptive nuclear first strike that could achieve decapitation of an adversary’s forces based on an ability to detect and track an incoming warhead with sufficient time to make a decision on retaliatory measures prior to receiving the first strike. HS/HM weapons shorten that decision timeline significantly such that an aggressing country may believe it has a greater chance of achieving a successful first strike, even if the reality is that these weapons are extremely unlikely to be manufactured in such quantity as to confidently prevent a retaliatory strike. Any country that possesses a belief, even if that belief is not based in reality, that it can win a nuclear war increases the probability of that country using these weapons in an offensive and coercive manner to achieve its objectives. This also lowers the threshold for the use of nuclear weapons in warfare.

An offensive and coercive posture, or the perception of such a posture enacted by one country is conducive to more aggressive defensive and offensive counter-posturing by another country. While it has been demonstrated that the development of HS/HM technology does not threaten the retaliatory capability of any of the great nuclear powers, the perceptions surrounding decisions to pursue such a program lead to misperception of intentions that appear to be aggressive and hostile, which in turn has the significant potential to destabilize the deterrence status quo.

Conclusions

Hypersonic/highly-maneuverable weapons represent a leap in the technological efficiency of nuclear delivery systems. These weapons travel at such a speed and possess a maneuverability to make them difficult to detect and track. However, due to the engineering difficulty and the materials needed, which drive a significant cost for such a program, it is highly unlikely that any country will manufacture these weapons in such a quantity as to threaten the current deterrence status quo. As a result, it is not the technology itself, but the perceptions of the intentions surrounding HS/HM programs that challenges the stability of the nuclear deterrence model. The lack of understanding of great nuclear power nations’ intentions regarding HS/HM weapons has the most potential to destabilize the deterrence status quo and lower the threshold for the use of nuclear weapons.

### Military---AT: Lockheed Solves---2AC

#### Their ev concedes global cooperation is the final barrier.

Partyard 22 – Partyard Military Division, worldwide supplier of OEM systems and aftermarket air, sea, and land spares and maintenance, 3/8/2022, "​​Why the World’s Militaries Are Embracing 5G," <https://partyardmilitary.com/2022/03/08/why-the-worlds-militaries-are-embracing-5g/>, RMax, condensed for readability

Warfare has always been carried out at the boundary between chaos and order. Strategists have long tried to suppress the chaos and impose order by means of intelligence, communication, and command and control. The most powerful weapon is useless without knowing where to aim it. The most carefully constructed plan leads nowhere if it is based on bad intelligence. And the best intelligence is worthless if it arrives too late. No wonder that over the past two centuries, as technologies such as photography, electronic communications, and computing became available, they were quickly absorbed into military operations and often enhanced by targeted defense R&D.

The next key enabler is fifth-generation (5G) wireless communications. The United States, Europe, China, and Russia are now integrating 5G technologies into their military networks. These are sizable and complicated projects, and several different strategies are already becoming apparent.

At Lockheed Martin, we’re enhancing standard 5G technologies to connect the many platforms and networks that are fielded by the various branches of the armed services. We call this our 5G.MIL initiative. Earlier this year, in two projects, called Hydra and HiveStar, we demonstrated the feasibility of key aspects of this initiative. Hydra yielded encouraging results on the interoperability challenge, and HiveStar showed that it was possible to quickly construct, in an area with no existing infrastructure, a highly mobile and yet capable 5G network, as would be required on a battlefield.

[their card ends]

The new work takes an unusual approach. It is a collaboration with commercial industry in which technology is transferred from the civilian to the military sector, not the other way around. Radar, rocketry, and nuclear energy got their starts in military labs, and it took years, even generations, for these technologies to trickle into consumer products. But today, for fundamental technologies such as computing and communications, the sheer scale of private-sector development is increasingly beyond the resources of even the largest national defense agencies. To deploy networks that are sufficiently fast, adaptive, agile, and interoperable, warfighters now have little alternative but to exploit commercial developments. No wonder, then, that the U.S. Department of Defense, through an initiative called 5G to NextG, and various complementary investments from individual armed services, has committed upwards of US $2 billion to advance commercial 5G research and to perform tests and experiments to adapt the results for military purposes. To understand the significance of such a shift, consider how the United States got to this juncture. In 18th-century conflicts, such as the Revolutionary War, the only battlefield sensors were human eyes and ears. Long-distance communication could take days and could be interrupted if the messengers it relied on were captured or killed. Tactical battlefield decisions were signaled by flags or runners to commence maneuvers or attacks. By World War II, combatants had radar, aircraft, and radios to sense enemy planes and bombers up to 80 miles ahead. They could communicate from hundreds of miles away and prepare air defenses and direct fighter-interceptor squadrons within minutes. Photoreconnaissance could supply invaluable intelligence—but in hours or days, not seconds. Today, the field of battle is intensively monitored. There are countless sensors on land, sea, air, space, and even in cyberspace. Jet fighters, such as the F-35, can act as information-processing hubs in the sky to fuse all that data into a single integrated picture of the battlefield, then share that picture with war fighters and decision makers, who can thus execute command and control in near real time. Three Lockheed Martin military aircraft, built in different eras, have different communications systems designed to make it hard for an adversary to detect a transmission. In a project called Hydra, engineers used electronic systems called open-system gateways to enable the three to communicate freely. From the top, the aircraft are the F-22, the U-2S, and the F-35. Lockheed Martin At least, that’s the goal. The reality often falls short. The networks that knit together all these sensors are a patchwork. Some of them run over civilian commercial infrastructure and others are military, and among the military ones, different requirements among the different branches and other factors have contributed to an assortment of high-performance but largely incompatible communication protocols. Messages may not propagate across these networks quickly or at all. Here’s why that’s a problem. Say that an F-35 detects an incoming ballistic missile. The aircraft can track the missile in real time. But today it may not be able to convey that tracking data all the way to antimissile batteries in time for them to shoot down the projectile. That’s the kind of capability the 5G.MIL initiative is aiming for. There are broader goals, too, because future battlefields will up the ante on complexity. Besides weapons, platforms, and gear, individual people will be outfitted with network-connected sensors monitoring their location, exposures to biochemical or radioactive hazards, and physical condition. To connect all these elements will require global mesh networks of thousands of nodes, including satellites in space. The networks will have to accommodate hypersonic systems moving faster than five times the speed of sound, while also being capable of controlling or launching cyberattacks, electronic warfare and countermeasures, and directed-energy weapons. Such technologies will fundamentally change the character and speed of war and will require an omnipresent communications backbone to manage capabilities across the entire battlefield. The sheer range of coordinated activities, the volume of assets, the complexity of their interactions, and their worldwide distribution would quickly overwhelm the computing and network capabilities we have today. The time from observation to decision to action will be measured in milliseconds: When a maneuvering hypersonic platform moves more than 3.5 kilometers per second, knowing its location even a second ago may be of little use for a system designed to track it. Our 5G.MIL vision has two complementary elements. One is exemplified by the opening scenario of this article: the quick, ad hoc establishment of secure, local networks based on 5G technology. The goal here is to let forces take sensor data from any platform in the theater and make it accessible to any shooter, no matter how the platform and the shooter each connect to the network. Aircraft, ships, satellites, tanks, or even individual soldiers could connect their sensors to the secure 5G network via specially modified 5G base stations. Like commercial 5G base stations, these hybrid base stations could handle commercial 5G and 4G LTE cellular traffic. They could also share data via military tactical links and communications systems. In either case, these battlefield connections would take the form of secure mesh networks. In this type of network, nodes have intelligence that enables them to connect to one another directly to self-organize and self-configure into a network, and then jointly manage the flow of data. Inside the hybrid base station would be a series of systems called tactical gateways, which enable the base station to work with different military communication protocols. Such gateways already exist: They consist of hardware and software based on military-prescribed open-architecture standards that enable a platform, such as a fighter jet made by one contractor, to communicate with, say, a missile battery made by another supplier. The second element of the 5G.MIL vision involves connecting these local mesh networks to the global Internet. Such a connection between a local network and the wider Internet is known as a backhaul. In our case, the connection might be on the ground or in space, between civilian and military satellites. The resulting globe-spanning backhaul networks, composed of civilian infrastructure, military assets, or a mixture of both, would in effect create a software-defined virtual global defense network. The software-defined aspect is important because it would allow the networks to be reconfigured—automatically—on the fly. That’s a huge challenge right now, but it’s critical because it would provide the flexibility needed to deal with the exigencies of war. At one moment, you might need an enormous video bandwidth in a certain area; in the next, you might need to convey a huge amount of targeting data. Alternatively, different streams of data might need different levels of encryption. Automatically reconfigurable software-defined networks would make all of this possible. The military advantage would be that software running on the network could use data sourced from anywhere in the world to pinpoint location, identify friends or foes, and to target hostile forces. Any authorized user in the field with a smartphone could see on a Web browser, with data from this network, the entire battlefield, no matter where it was on the planet. We partnered recently with the U.S. Armed Services to demonstrate key aspects of this 5G.MIL vision. In March 2021, Lockheed Martin’s Project Hydra demonstrated bidirectional communication between the Lockheed F-22 and F-35 stealth fighters and a Lockheed U-2 reconnaissance plane in flight, and then down to ground artillery systems. This latest experiment, part of a series that began in 2013, is an example of connecting systems with communications protocols that are unique to their mission requirements. All three planes are made by Lockheed Martin, but their different chronologies and battlefield roles resulted in different custom communications links that aren’t readily compatible. Project Hydra enabled the platforms to communicate directly via an open-system gateway that translates data between native communications links and other weapons systems. Emerging technologies will fundamentally change the character and speed of war and will require an omnipresent communications backbone to manage capabilities across the entire battlefield. It was a promising outcome, but reconnaissance and fighter aircraft represent only a tiny fraction of the nodes in a future battle space. Lockheed Martin has continued to build off Project Hydra, introducing additional platforms in the network architecture. Extending the distributed-gateway approach to all platforms can make the resulting network resilient to the loss of individual nodes by ensuring that critical data gets through without having to spend money to replace existing platform radios with a new, common radio. Another series of projects with a software platform called HiveStar showed that a fully functional 5G network could be assembled using base stations about the size of a cereal box. What’s more, those base stations could be installed on modestly sized multicopters and flown around a theater of operations—this network was literally “on the fly.” The HiveStar team carried out a series of trials this year culminating in a joint demonstration with the U.S. Army’s Ground Vehicle Systems Center. The objective was to support a real-world Army need: using autonomous vehicles to deliver supplies in war zones. The team started simply, setting up a 5G base station and establishing a connection to a smartphone. The base-station hardware, a gNodeB in industry parlance, was an OctNode2, from Octasic in Montreal. The base station weighs about 800 grams and measures about 24 × 15 × 5 centimeters. A white 3-D printed box housed processors for distributed-computing and communications software, called HiveStar. The housings were mounted on unpiloted aerial vehicles for a demonstration of a fully airborne 5G network.Lockheed Martin The team then tested the compact system in an area without existing infrastructure, as might very well be true of a war zone or disaster area. The team mounted the gNodeB and a tactical radio operating in the S band on a DJI Matrice 600 Pro hexacopter and flew the package over a test range at Lockheed Martin’s Waterton, Colo., facility. The system passed the test: It established 5G connectivity between this roving cell tower in the sky with a tablet on the ground. Next, the team set about wirelessly connecting a group of base stations together into a flying, roving heterogeneous 5G military network that could perform useful missions. For this they relied on Lockheed-Martin developed software called HiveStar, which manages network coverage and distributes tasks among network nodes—in this case, the multicopters cooperating to find and photograph the target. This management is dynamic: if one node is lost to interference or damage, the remaining nodes adjust to cover the loss. For the team’s first trial, they chose a pretty standard military chore: locate and photograph a target using multiple sensor systems, a function called tip and cue. In a war zone such a mission might be carried out by a relatively large UAV outfitted with serious processing power. Here the team used the gNodeB and S-band radio setup as before, but with a slight difference. All 5G networks need a software suite called 5G core services, which is responsible for such basic functions as authenticating a user and managing the handoffs from tower to tower. In this trial, those core functions were running on a standard Dell PowerEdge R630 1U rack-mounted server on the ground. So the network consisted of the gNodeB on the lead copter, which communicated with the ground using 5G and depended on the core services on the ground computers. The lead copter communicated using S-band radio links, with several camera copters and one search copter with a software-defined radio programmed to detect an RF pulse in the target frequency. The team worked with the HiveStar software, which managed the network’s communications and computing, via the 5G tablet. All that was needed was a target for the copters to search for. So the team outfitted a remotely controlled toy jeep, about 1 meter long, with a software-defined radio emitter as a surrogate target. The team initiated the tip-and-cue mission by entering commands on the 5G tablet. The lead copter acted as a router to the rest of the heterogeneous 5G and S-band network. Messages initiating the mission were then distributed to the other cooperating copters via the S-band radio connection. Once these camera platforms received the messages, their onboard HiveStar mission software cooperated to autonomously distribute tasks among the team to execute search maneuvers. The multicopters lifted off in search of the target RF emitter. Once the detecting copter located the target jeep’s radio signal, the camera copters quickly sped to the area and captured images of the jeep. Then, via the 5G gNodeB, they sent these images, along with precise latitude and longitude information, to the tablet. Mission accomplished. Next the team thought of ways to fly the entire 5G system, freeing it from any dependence on specific locations on the ground. To do this, they had to put the 5G core services on the lead copter, the one outfitted with the gNodeB. Working with a partner company, they loaded the core services software onto a single board computer, an Nvidia Jetson Xavier NX, along with the gNodeB. For the lead copter, which would carry this gear, they chose a robust, industrial-grade quadcopter, the Freefly Alta X. They equipped it with the Nvidia board, antennas, filters, and the S-band radios. At the Army’s behest, the team came up with a plan to use the flying network to demonstrate leader-follower autonomous-vehicle mobility. It’s a convoy: A human drives a lead vehicle, and up to eight autonomous vehicles follow behind, using routing information transmitted to them from the lead vehicle. Just as in the tip-and-cue demonstration, the team established a heterogeneous 5G and S-band network with the upgraded 5G payload and a series of supporting copters that formed a connected S-band mesh network. This mesh connected the convoy to a second, identical convoy several kilometers away, which was also served by a copter-based 5G and S-band base station. After the commander initiated the mission, the Freefly Alta X flew itself above the lead vehicle at a height of about 100 meters and connected to it via the 5G link. The HiveStar mission-controller software directed the supporting multicopters to launch, form, and maintain the mesh network. The vehicle convoy started its circuit around a test range about 10 km in circumference. During this time, the copter connected via 5G to the lead convoy vehicle would relay position and other telemetric information to the other vehicles in the convoy, while following overhead as the convoy traveled at around 50 km per hour. Data from the lead vehicle was shared by this relay to following vehicles as well as the second convoy via the distributed multicopter-based S-band mesh network. Illustration of satellites and other elements and how they are all connected. Current 5G standards do not include connections via satellites or aircraft. But planned revisions, designated Release 17 by the 3rd Generation Partnership Project consortium, are expected next year and will support nonterrestrial networking capabilities for 5G.Chris Philpot The team also challenged the system by simulating the loss of one of the data links (either 5G or S-band) due to jamming or malfunction. If a 5G link was severed, the system immediately switched to the S band, and vice versa, to maintain connectivity. Such a capability would be important in a war zone, where jamming is a constant threat. Though encouraging, the Hydra and HiveStar trials were but first steps, and many high hurdles will have to be cleared before the scenario that opens this article can become reality. Chief among these is expanding the coverage and range of the 5G-enabled networks to continental or intercontinental range, increasing their security, and managing their myriad connections. We are looking to the commercial sector to bring big ideas to these challenges. Satellite constellations, for instance, can provide a degree of global coverage, along with cloud-computing services via the internet and the opportunity for mesh networking and distributed computing. And though today’s 5G standards do not include space-based 5G access, the Release 17 standards coming in 2022 from the 3rd Generation Partnership Project consortium will natively support nonterrestrial networking capabilities for the 5G ecosystem. So we’re working with our commercial partners to integrate their 3GPP-compliant capabilities to enable direct-to-device 5G connectivity from space. In the meantime, we’re using the HiveStar/multicopter platform as a surrogate to test and demonstrate our space-based 5G concepts. Security will entail many challenges. Cyberattackers can be counted on to attempt to exploit any vulnerabilities in the software-defined networking and network-virtualization capabilities of the 5G architecture. The huge number of vendors and their suppliers will make it hard to perform due diligence on all of them. And yet we must protect against such attacks in a way that works with any vendor’s products rather than rely, as in the past, on a limited pool of preapproved solutions with proprietary (and incompatible) security modifications. The advent of ultrafast 5G technology is an inflection point in military technology. Another interesting little challenge is presented by the 5G waveform itself. It’s made to be easily discovered to establish the strongest connection. But that won’t work in military operations where lives depend on stealth. Modifications to the standard 5G waveform, and how it’s processed within the gNodeB, can achieve transmission that’s hard for adversaries to pick up.

Perhaps the greatest challenge, though, is how to orchestrate a global network built on mixed commercial and military infrastructure. To succeed here will require collaboration with commercial mobile-network operators to develop better ways to authenticate user connections, control network capacity, and share RF spectrum. For software applications to make use of 5G’s low latency, we’ll also have to find new, innovative ways of managing distributed cloud-computing resources.

It’s not a leap to see the advent of ultrafast 5G technology as an inflection point in military technology. As artificial intelligence, unpiloted systems, directed-energy weapons, and other technologies become cheaper and more widely available, threats will proliferate in both number and diversity. Communications and command and control will only become more important relative to more traditional factors such as the physical capabilities of platforms and kinetic weapons. This sentiment was highlighted in the summary of the 2018 U.S. National Defense Strategy, the strategic guidance document issued every four years by the U.S. DOD: “Success no longer goes to the country that develops a new technology first, but rather to the one that better integrates it and adapts its way of fighting.”

Here, it is worth noting that Chinese companies are among the most active in developing 5G and emerging 6G technologies. Chinese firms, notably Huawei and ZTE Corp., have more than 30 percent of the worldwide market for 5G technology, similar to the combined market shares of Ericsson and Nokia. Chinese market share could very well increase: According to the Council on Foreign Relations, the Chinese government backs companies that build 5G infrastructures in countries China invests in as part of its Belt and Road Initiative. Meanwhile, in Europe, NATO unveiled its first 5G military test site in Latvia in 2020. Norway, notably, is exploring dedicating software-defined networks in commercial 5G infrastructure to support military missions.

Perhaps this convergence of commercial and defense-sector development around 5G, 6G, and future communications technologies will lead to powerful and unexpected commercial applications. The defense sector gave the world the Internet. The world now gives militaries 5G communications and beyond. Let’s find out what the defense sector can give back.

### Military---AT: NC3 D---2AC

#### NC3 entanglement causes escalation.

Herbert Lin 21, senior research scholar for cyber policy and security at the Center for International Security and Cooperation and fellow in Cyber Policy at the Hoover Institution, “Cyber Risk Across the U.S. Nuclear Enterprise,” *Texas National Security Review*, Vol. 4, Issue 3, <https://repositories.lib.utexas.edu/bitstream/handle/2152/87036/TNSRVol4Issue3Lin.pdf>, RMax

Scenarios Involving Cyber-Driven Pathways to Nuclear Crisis

To illustrate what is at stake if cyber risks are not adequately addressed, below are several nuclear scenarios in which cyber attacks by one side on the other might have a real and tangible effect on the the likelihood of nuclear use.

A first scenario involves differing perceptions of cyber penetrations of NC3 during a nuclear crisis. Cyber attacks and cyber espionage/intelligence gathering (cyber exploitation) use the same penetration techniques and differ only in what they seek to accomplish. Thus, any given cyber penetration carries with it an unknown potential for both attack and exploitation. A cyber penetration from nation A detected in nation B’s NC3 system could be part of a relatively benign attempt to gather intelligence. Or it could be the start of a serious cyber attack. It is impossible for nation B to know nation A’s intentions before the payloads are executed. A worst-case assessment would regard A’s penetration as the start of an attack on B’s NC3 system.28

A second scenario could arise when a nation chooses to combine (that is, to entangle) nuclear C3 and conventional C3 functions on the same technology platforms and take advantage of the same command, control, and communications infrastructure for reasons of economy. During the initial stages of a conflict, nation A may target nation B’s conventional C3 infrastructure for the understandable and militarily justified purpose of degrading B’s conventional combat power. But if the technological infrastructure for both conventional and nuclear C3 is the same, such an attack could actually degrade B’s nuclear C3 capabilities as well as give rise to concerns that A is deliberately trying to degrade B’s nuclear capabilities preemptively.29

A third scenario stems from the fact that offensive cyber capabilities are usually concealed out of a concern that, if revealed, an adversary will be able to negate those capabilities.30 If nation A is able to penetrate nation B’s nuclear enterprise clandestinely, A has the advantage over B without B realizing it. In a crisis, A knows it has the upper hand over B and feels no need to refrain from escalation. However, B does not know about the penetration, and, believing itself to be as strong as it ever was, does not know that it would be wise to refrain from escalation. Each side’s unwillingness to refrain from escalation creates more risk for the other side.

A fourth scenario has to do with using cyber attacks to damage an adversary’s confidence in its nuclear capabilities. Seeking to compromise an adversary’s nuclear deterrent and exploiting vulnerabilities in its supply chains, nation A places malware (or hardware vulnerabilities) on a number of nation B’s nuclear delivery platforms. During an escalating crisis, A communicates to B what it has done and demonstrates that it has done so by providing clues that allow B to discover these vulnerabilities. A then informs B that it has done this on many more of B’s platforms. B now must consider how to react as it tries to determine what is mere boasting and which of B’s platforms have been genuinely compromised.

### Military---AT: NC3 D---Offline---2AC

#### The entire NC3 system is being modernized.

Herbert Lin 21, senior research scholar for cyber policy and security at the Center for International Security and Cooperation and Hank J. Holland Fellow in Cyber Policy and Security at the Hoover Institution, both at Stanford University, Summer 2021, “Cyber Risk Across the U.S. Nuclear Enterprise”, <https://tnsr.org/2021/06/cyber-risk-across-the-u-s-nuclear-enterprise/>

Substantial efforts are being and will be made to modernize the NC3 system. According to the Congressional Research Service, NC3 modernization is likely to include new early-warning radars, new infrared early-warning satellites, new communications satellites, and replacements for the E4-B airborne command posts and E6-B communications relay aircraft.[17](https://tnsr.org/2021/06/cyber-risk-across-the-u-s-nuclear-enterprise/" \l "_ftn17) But just as importantly, new nuclear delivery systems and platforms will be “much more like all systems today, network connected. They’ll be cyber enabled” and will have “some level of connectivity to the rest of the warfighting system,” according to Werner J. A. Dahm, chair of the Air Force Scientific Advisory Board.[18](https://tnsr.org/2021/06/cyber-risk-across-the-u-s-nuclear-enterprise/" \l "_ftn18) The significance of being “cyber-enabled” is hard to overstate. Adm. Cecil Haney, former commander of U.S. Strategic Command, testified in 2014 that “We are working to shift from point-to-point hardwired systems to a networked IP-based national C3 architecture.”[19](https://tnsr.org/2021/06/cyber-risk-across-the-u-s-nuclear-enterprise/" \l "_ftn19) The shift to “cyber-enabled” connectivity will mean a higher degree of interoperability among NC3 components, which will no longer be as constrained by hardware restrictions.

# Topicality

## Cybersecurity

### T-CIA---WM---2AC

#### We meet – 5G cybersecurity is vital to the CIA triad

Leleux et al ’21 [Darrin, Deputy Director of the Electromagnetic Spectrum Operations Cross-Functional Team earned his Master of Science in Computer Engineering from the University of Houston at Clear Lake in 1998, and a PhD in Electrical Engineering from Rice University in 2002, Winter 2021, “Fifth Generation Wireless Development in Great Power Competition,” Cyber Defense Review, <https://cyberdefensereview.army.mil/Portals/6/Documents/2021_winter_cdr/02_CDR_Winter_2021_Leleux.pdf?ver=X83q7TOOVMvhrIJHxhBw_A%3D%3D>, St. Mark’s, AM]

Security standards provide the basic parameters to create a secure environment across 5G wireless networks and are vital to maintain the confidentiality, integrity, and availability of US data as it traverses through information networks. To protect US data and systems, several improvements to current systems need to be pursued, including policy changes to ensure only secure equipment is used in USG systems, the development of quantum-resistant cryptography, improvement of software-defined networking technologies, and tighter controls over supply chain management. All these changes must be carefully orchestrated to work in concert with each other across all government agencies and industry partners.

### T-Cyber---AT: Not Cybersecurity---2AC

#### 5G requires cybersecurity.

Bala Sethunathan 22, Director, Security Practice & CISO, 1-18-22, "5G and Cybersecurity: All You Need to Know," SoftwareONE, <https://www.softwareone.com/en-us/blog/all-articles/2022/01/17/5g-and-cybersecurity-all-you-need-to-know> //billy

For every positive business outcome that 5G brings, it also has an equal and opposite cybersecurity risk. Here are a few known risks:

IoT exposure

Companies need to adopt IoT devices as part of their business strategies, but they come with inherent security vulnerabilities, like misconfigurations and lack of standardized security practices. The same 5G high-speed, low-latency connections that provide value for the enterprise also give cybercriminals a way to rapidly execute network attacks.

Some examples of attacks that leverage insecure IoT devices include:

Botnets

Distributed denial of service (DDoS)

Man-in-the-middle

Call interception and location tracking

Compromised Network Slice

Network slicing helps enable security, but its complexity can lead to insecure implementations. Currently, network administrators are on their own trying to implement these new networking architectures.

Without standards or guides, network administrators may not be able to build the appropriate security into their implementations, accidentally giving cybercriminals a way to gain unauthorized access to the network slice. For example, cybercriminals can compromise the network by leveraging this attack vector then use it as a steppingstone to data breaches or DDoS attacks.

Stretched Security Monitoring Resources

As 5G expands the number of devices that can connect to networks, it increases the amount of security resources needed to monitor these new access points. Adding more IoT devices to the organization’s infrastructure enables productivity and efficiency, but every device needs to be monitored continuously.

# Counterplans

## General

### Cyber Key---2AC

#### 5G increases vulnerabilities---ensuring cybersecurity is key

Katarina Kertysova 21, Policy Fellow at the European Leadership Network, Global Fellow at the Wilson Centre, 2/25/2021, “When 5G Meets AI: Next Generation of Communication and Information Sharing,” *NATO Strategic Communications Centre of Excellence*, <https://stratcomcoe.org/publications/when-5g-meets-ai-next-generation-of-communication-and-information-sharing/237>, RMax

Cyber (in)security

5G is generally considered more secure than previous networks (2G, 3G, 4G LTE) due to better encryption58 and the ability for network slicing, which makes potential breaches less likely and less damaging.59 Since 5G is an evolution of 4G LTE, developers of this technology have been able to deal with weaknesses and vulnerabilities in previous networks and build security improvements into the protocol to ensure that 5G is more secure. However, that potential for extra security may not be delivered by the service providers for cost reasons. Despite increasing risk, not all manufacturers prioritize cybersecurity. Perhaps the greatest risk concerns extension of the attack surface. As connected devices proliferate in a 5G environment, the threat potential as well as new points of attack increase. Put simply, any system is only as strong as its weakest link: billions of interconnected devices with varied security also mean billions of possible breach points.60 Given 5G’s edge computing potential, this is a concern for the creators of 5G infrastructure and networks across Europe.

Most of the attention surrounding the cybersecurity of 5G networks has focused on supply chain challenges. Chinese companies currently lead in 5G development and Huawei dominates the global market for telecommunications equipment. In 2019, twothirds of 5G networks outside China relied on telecom equipment manufactured in China.61 On top of reported security vulnerabilities – such as software code deficiencies or poor oversight of its supplier networks – which could be exploited by any malign actor, concerns have also been voiced about Huawei’s ties to the Chinese government and the potential risk that China might use 5G infrastructure for espionage or illicit actions (such as intellectual property theft, company sabotage, or fraud).62 The Chinese State Security Law obliges companies to ‘provide assistance with work related to state security’.63 If critical communications, including Internet voting, come to depend on 5G networks, this will create a level of insecurity since the Chinese regime might gain access to and eventually manipulate such processes.64 The ability to manipulate public opinion, with implications for democracy, is certainly there, just like it was with 4G. With 5G, however, the lack of trust in its architecture, alongside uncertainties about how the infrastructure operates, heightens some of those concerns.

In addition to user profiling and political microtargeting, with the roll-out of 5G, an increase in the volume and speed of data theft is expected.65 As confirmed by the US Cybersecurity and Infrastructure Security Agency (CISA), 5G networks will constitute ‘an attractive target for criminals and foreign adversaries to exploit for valuable information and intelligence’.66

#### Cybersecurity is key winning the 5G race.

Tom Wheeler 19, visiting fellow in Governance Studies at The Brookings Institution, former Chairman of the FCC; and David Simpson, Professor at the Pamplin College of Business at Virginia Tech, Former Chief of Public Safety and Homeland Security Bureau at the FCC, 2019, “Why 5G Requires New Approaches to Cybersecurity,” *The Global Race for Technological Superiority: Discover the Security Implications*, <https://www.ispionline.it/it/pubblicazione/global-race-technological-superiority-discover-security-implications-24463>, RMax

“The race to 5G is on and America must win”, President Donald Trump said in April1 . For political purposes, that “race” has been defined as which nation gets 5G built first. It is the wrong measurement.

The United States and Europe must “fire first effectively” in their deployment of 5G. Borrowing on a philosophy Admiral Arleigh Burke coined in World War II: Speed is important, but speed without a good targeting solution can be disastrous2.

5G will be a physical overhaul of essential networks that will have decades-long impact. Because 5G is the conversion to a mostly all-software network, future upgrades will be software updates much like the current upgrades to smartphones. Because of the cyber vulnerabilities of software, the tougher part of the real 5G “race” is retooling how to secure the most important network of the XXI century and the ecosystem of devices and applications that sprout from that network.

Beyond the vulnerabilities of software, 5G networks have another vulnerability: a supply chain that circles the world. From hardware, software and firmware to the design of the apps and devices using the network, the 5G supply chain is composed of numerous participants. Each of these participants rely on the others, but none has cybersecurity as their core responsibility.

The new capabilities made possible by new applications riding 5G networks hold tremendous promise. As the United States and Europe pursue the connected future, however, they must place equivalent – if not greater – focus on the security of those connections, devices, and applications. To build 5G on top of a weak cybersecurity foundation is to build on sand. This is not just a matter of the safety of network users, it is a matter of national security – and a geopolitical imperative.

### NATO Key---2AC

#### NATO is key to ensure that the next generation of 5G technology is used for military purposes

Machi 22 [Vivienne Machi is a reporter based in Stuttgart, Germany, contributing to Defense News' European coverage. She previously reported for National Defense Magazine, Defense Daily, Via Satellite, Foreign Policy and the Dayton Daily News. She was named the Defence Media Awards' best young defense journalist in 2020;"NATO wants a say in 5G standardization talks"; 3-22-2022; Federal Times; [Hyperlinked here because it's really long](https://www.federaltimes.com/battlefield-tech/it-networks/5g/2022/03/22/nato-wants-a-say-in-5g-standardization-talks/?contentQuery=%7B%22section%22%3A%22%2Fhome%22%2C%22exclude%22%3A%22%2Fglobal%2Feurope%22%2C%22from%22%3A55%2C%22size%22%3A10%7D&contentFeatureId=f0fmoahPVC2AbfL-2-1-8)]//AShah

STUTTGART, Germany – NATO’s technical agency wants to make sure it has a say in ongoing 5G standardization talks to ensure the critical technology can be used for both civilian and military purposes.

For Antonio Calderon, interim chief technology officer for the NATO Communication and Information Agency (NCIA), fifth-generation wireless technology has the potential to enable swaths of novel capabilities for the defensive alliance.

That’s why it’s important that NCIA have a voice in ongoing discussions about 5G standardization, he said in an interview with Defense News. If two NATO member nations went into a maritime exercise with capabilities that used a future, currently hypothetical, NATO 5G standard, those nations would be able to securely communicate without the use of a base station.

The agency is in ongoing conversations with industry partners with connections to the 3rd Generation Partnership Project (3GPP), the umbrella term for a number of organizations that develop protocols for mobile communications.

“We don’t have a seat in that 3GPP, but we can raise our concerns” with the members, Calderon said. “If we are not part of that discussion, if we are not around the table, the 5G standards will be focused on civilian applications.”

That would be a drawback to NATO and its partners, who see a huge opportunity for 5G to provide next-generation connectivity and enhanced network management to troops across domains. Calderon, who prior to joining NATO worked in the civilian telecommunications industry, noted that if industry comes up with its own 5G standard without considering military-specific features, they run the risk of narrowing their business case.

For the past several years, the agency has been conducting internal technical assessments to evaluate the potential of 5G for military applications.

NCIA has pared down its focus from four to two specific applications: for maritime communications and for deployable communications and information systems (CIS), Calderon said. Those two applications were chosen due to the maturity of their technology and their potential in the civilian domain as well as military, he added.

“Those two already have a mature industry, doing trials and proofs of concept,” he said. “But those two are also the most interesting for NATO – it’s hand in hand.”

The alliance has recently established its own multinational 5G initiative, with over 10 member-nations currently involved. The initiative is in its early stages, and the member nations are determining how best to contribute to the 5G efforts – whether financially, in-kind with experts or engineers, or a combination.

Calderon said NCIA has currently dedicated funding “in the single millions” for 5G technologies, but noted that if the 5G initiative materialized into a “real program,” they could dedicate ten times more funding than that. The agency may also be able to tap into [NATO’s recently established technology accelerator,](https://www.defensenews.com/global/europe/2021/06/22/nato-hopes-to-launch-new-defense-tech-accelerator-by-2023/)the Defense Innovation Accelerator of the North Atlantic (DIANA).

By 2023, NATO hopes for DIANA to have established links with test centers across its member nations to help validate, test and co-design emerging and next-generation technologies. “5G could be a good candidate for one of those defense challenges that maybe DIANA … could address,” Calderon said.

But in the meantime, NATO will continue to work to ensure the military uses of 5G are taken into account in the civilian development of new standards, he added.

“Then, the products will have those standards that are really useful … and valuable for us,” he said.

### NATO Key---1AR

#### NATO key - ensures the US and Europe don’t drift, which deters China and means Huawei does not compromise NATO information sharing.

Larsen ’22 (Henrik Larsen, Ph.D., senior researcher at the Center for Security Studies at the Swiss Federal Institute of Technology Zurich. “NATO Must Get Resilience Right to Withstand Russia and China” 05/22/22 <https://www.lawfareblog.com/nato-must-get-resilience-right-withstand-russia-and-china>) ☺

China does not compare to the direct threat that Russia poses but has nevertheless appeared on NATO’s strategic radar as an economic great power with a high-tech edge that Russia is unlikely to ever match. Chinese 5G network provider Huawei remains a pertinent topic for NATO, as several European countries, including Germany, Austria, Spain, the Netherlands and Hungary, are still undecided about relying on its potentially compromised technology or de facto allowing their national operators to use Chinese providers. Moreover, Chinese investments in continental Europe without conditionalities attached and targeting critical infrastructure (railway stations, ports and airports) raise suspicions about Beijing’s underlying political and military motives. Moreover, China is pressing ahead with military applications of artificial intelligence (AI), and its space ambitions are growing.

Since 2014, NATO has become increasingly aware of the nonmilitary challenges to its unity and resilience but has adapted only in certain respects. It adopted the so-called baseline requirements in 2016, against which it can measure individual allies’ level of resilience regarding their provision of essential services to their domestic populations. These basics that would be necessary to withstand a crisis include access to food, water and energy supplies; maintenance of core functions of government; and resilient civil transportation systems. However, the baseline requirements are technical measurements that do not adequately grasp the political nature of the challenges that Russia and China pose to alliance unity. Moreover, their focus on civil preparedness, resource management and infrastructure does not seem to fit squarely within the competencies of a defense alliance. NATO may be on a slippery slope with the scope of its resilience concept drifting further away from its defense capabilities.

NATO, as an organization and as an alliance of states, is aware of the challenges to transatlantic resilience and cohesion that Russia and China pose, but the alliance has not been able to agree on the issues to which it can bring added value. The situation today stands in contrast to the situation during the Cold War when NATO successfully calibrated resilience to the ability to resist an armed attack by focusing on civil emergency planning. Russia and China are illiberal challengers that add new meaning to transatlantic security cooperation, but NATO’s adaptation will depend on the extent to which the United States and Europe can find agreement on investment in transatlantic security.

U.S. and European Perspectives

From the U.S. perspective, the rise of China compels a harsher foreign policy prioritization that delegates more responsibilities to European states. President Biden was elected on the promise of a “foreign policy for the middle class,” which was an effort to win back some of the Trump voters dissatisfied with the United States paying the bill for transatlantic defense. The refocus on the U.S. domestic base has so far manifested itself in the precipitous withdrawal from Afghanistan and the clumsy diplomatic handling of the announcement of the security pact among Australia, the United Kingdom and the United States. These two decisions give Europeans reason to question the durability of U.S. leadership beyond President Trump.

It took Russia’s invasion of Ukraine for the Biden administration to play a major role in European security, which has been exercised in terms of economic sanctions against Russia and arms supplies to Ukraine. Biden’s declaration to his allies that “America is back” after assuming office had until then yielded little concrete results. Unlike its predecessor, the Biden administration is not obsessed with numerical defense spending and understands security more broadly in terms of the capacity to defend against illiberal threats. Washington expects the Europeans to be reliable allies in the competition with Russia and China, but it has not specified which functions it wishes NATO to perform.

From a European perspective, Russia’s invasion of Ukraine marks a new reality of increased defense spending that will likely redress some of the military imbalance between the United States and European NATO allies since the end of the Cold War. It is positive that the United States seeks cooperation on a wider array of security issues, such as trade and technology, that are core to a resilient and united transatlantic alliance. At the same time, it is continental Europe, not North America and the United Kingdom, that risks emerging as a weak transatlantic link under growing Russian and Chinese influence and, therefore, must make the necessary adjustment.

The vagueness of U.S. expectations and the questionable durability of U.S. leadership seems to give European allies more leverage in defining the alliance’s strategic outlook on resilience. Restricting nontrusted technology and economic investments and fighting foreign subversion are mostly national decisions, but the European Union has exclusive powers with regard to trade and coordinates significant assets in other areas. The European allies can shape the U.S. push for NATO’s functional expansion by clarifying four areas in which the alliance can add value to transatlantic resilience.

Four Areas of Adaptation

First, NATO needs to make clear the aspects of resilience for which it is not placed to lead. As a rule, the more NATO engages the civilian aspects of security, the more it moves away from its mandate. The alliance seems to have no natural role in law enforcement—such as fighting foreign influence operations or weaponized corruption—because of the variety in allied legislative frameworks and the existence of other established channels for ordinary police cooperation. NATO may be able to play a bigger role in coordinating between intelligence services on counterterrorism (against Russia) and counterintelligence (both Russia and China). The challenges arising from disinformation are real, as seen during the Russian invasion of Ukraine, but NATO has no role in countering foreign efforts to undermine public trust in the functioning of democratic institutions in its allies. The alliance should confine its anti-disinformation efforts to military affairs and Russian attempts to depict the alliance as an aggressor and a violator of the agreements that brought the Cold War to an end.

Second, NATO needs to identify which aspects of resilience it is positioned to lead. The most pertinent issue seems to be reducing Russian temptations to destabilize its eastern territory, notably Estonia and Latvia with significant Russian-speaking minorities, and the Lithuanian-Polish border toward the Kaliningrad exclave. Russia-instigated gray zone conflict on NATO territory seems more likely than a large-scale conventional war, especially given the poor performance of Russian forces in Ukraine. Russia still prefers to rely on disinformation and subversion to stir ethnic and political discord and may also return to using special operations incursions as a destabilization strategy, as it did during its seizure of Crimea in 2014. NATO needs to deter Russia across multiple domains of warfare by structuring and training a part of its future forces for gray zone eventualities that may precede Russia’s application of large-scale kinetic force. Integrating preparations to combat gray zone tactics into NATO’s conventional planning would allow it to implement a stronger, more crisis-ready resilience concept. NATO’s cyber defense capabilities are obviously relevant against Russian attempts to disrupt allied or national functions that may precede a conventional attack. And NATO should also work to deny hostile powers the capacity to neutralize or jam NATO and reconnaissance satellites.

Third, NATO must position itself to counter the rise of China. Although official NATO rhetoric refers to the protection of the rules-based international order, its mandate centers geographically on the Euro-Atlantic area and not the Asia-Pacific. Other than reasserting the general differences between China’s autocratic approach to the use of personal data and public-private relationships and those of NATO allies, NATO has no role in regulating transatlantic trade. The alliance may recognize Chinese acquisitions of critical infrastructure in Europe as a vulnerability to force mobility in a crisis, as well as Chinese 5G technology as an obstacle to allied information-sharing, without pretense to its ability to influence the economic choices of allied governments. Conversely, NATO has a distinct role in ensuring interoperability and the development of common principles for the responsible use of AI and other so-called emerging and disruptive technologies. NATO allies consider AI valuable for logistics and intelligence but, unlike China, are opposed to lethal uses without human authorization. China’s technological advances create pressure on NATO to ensure that North America and Europe do not drift apart in terms of interoperability and regulatory approaches to future war technology. China’s growing capabilities in cyberspace and outer space offer NATO an additional role in military threat definition and integration into allied structures and operational procedures.

#### NATO has to develop a strategy to map out risk and adequate response to cyber threats on 5G systems as recommended by military experts

Civitta 22 [Civitta provides management consulting and data analytics services to corporations, start-ups, SMEs, governments and NGO; "Military Movement: Risks from 5G Networks"; xx-xx-22; https://ccdcoe.org/uploads/2022/06/Report\_Military-Movement-Risks-from-5G-Networks.pdf]//AShah

DEVELOP A COMPREHENSIVE 5G CYBERSECURITY STRATEGY | As the military will interact with the rapidly developing 5G ecosystem, NATO will have to develop a comprehensive cybersecurity strategy by mapping out the various forms of interactions, corresponding risks, and adequate responses. In the strategy, all military movement needs must be identified, infrastructure enabling the movement must be mapped and its technological composition evaluated. Based on that mapping, all the opportunities and risks related to the intersection of future military movement and 5G development should be highlighted with recommendations developed by military and technological experts. The strategy would facilitate making Alliance-wide strategic decisions regarding 5G-use, including recommendations to private 5G network owners and intelligent transportation system providers. Given that security management will become essential in handling ongoing threats and risks, a proactive plan for the security management cannot be developed before a comprehensive cybersecurity strategy is in place.

#### NATO and other military stakeholders must engage in a process of discussion and communication to align interests and ensure interoperability

Bastos et al 20 [Luis Bastos is a Senior Scientist, CIS at NATO C3 Agency, Germano Capela is a scientist at the NATO Communications and Information Agency, Alper Koprulu is a scientist at the NATO Communications and Information Agency; 09-15-2020; https://www.mindev.gov.gr/wp-content/uploads/2020/11/Enclosure-2-Working-paper-Potential-of-5G-technologies-for-military-application.pdf]//AShah

VIII. RECOMMENDATIONS Based on the conclusions above, we recommend military communications stakeholders at NATO and nations the following: 1) Organize a workshop with military communications stakeholders on 5G to discuss ideas, collect inputs, and synchronize findings. Different communities and teams across the military communities are looking at the potential and challenges of 5G from different angles. In this context, it is pertinent to organize an informal discussion to synchronize views and collect inputs to discuss interim results, identified opportunities, initial reference 5G military scenarios, and collect additional inputs, to prepare follow-on engagements with other stakeholders including industry. In this discussion, it is also critical to involve multiple communities of interest (i.e., Cyber, Intelligence, Command and Control and Core Services). 2) Conduct comprehensive assessments of 5G for military application. Given the complexity of the topic (see Conclusion 1), the evolving standardization activities, the different potential implementation domains and variables, and the immaturity of some 5G features, the credible investigation of 5G and related technologies for military application requires a significant and stable effort to be conducted by a technical team, which is only possible with a robust and relatively long-term involvement. 3) Engage with the military communications industry to assess the state of the art in 5G developments and discuss implementation challenges in military scenarios. The initial reference 5G military scenarios highlighted in this paper have identified a myriad of implementation challenges (in [2]) for the associated technical concepts on the use of private or public 5G systems in NATO/military scenarios. In ad-hoc contacts with 5G industry and operators, the authors also noted a number of ongoing R&D activities in different laboratories to assess experimental 5G technologies and applications. Therefore, it highly recommended that military representatives and scientists engage with these communities to obtain first-hand feedback on the implementation challenges associated with some reference military 5G scenarios. 4) Publish a technical paper in a credible military communications conference. In order to facilitate informed dialogues with stakeholders on military applications/use of 5G technologies and systems, as well as to raise awareness to the potential and associated implementation challenges of some concepts, it is key to bring awareness to the topic and to communicate it to a wide audience. Publishing a concept paper on the initial opportunities and challenges of military applications of 5G technologies in the form of a credible technical paper facilitates this effort and contributes to informed discussions with a large audience. 5) In assessing the potential of 5G, assess also the potential of related wireless technologies. 5G is highly related to other technologies both at the Radio Access Network (RAN) and at the Data Network levels. Specifically, the 5G RAN has an open architecture to include the integration with other wireless access technologies (e.g., LTE Advanced, WLAN technologies, NTN-based 5G). In turn, some these non-5G wireless technologies4 may bring significant benefits to some military applications and should be also addressed. 6) Invest in monitoring, participating and contributing to 3GPP's work plan. As per stated in Conclusion 3, 3GPP is the forum where 5G requirements and specifications are discussed and agreed. Having military representatives participating at 3GPP would ensure that military interests are better represented and would provide the informed inputs to civil participants interested in military/public safety applications. NATO scientists could play this role and represent NATO/military interests at 3GPP. 7) Consider developing a multi-stakeholder effort to exploit the potential of 5G and other civil high-performance wireless technologies in support of military applications. Given the need to conduct significant work to effectively assess the potential of 5G and related technologies for effective military applications, it is recommended that NATO and national stakeholders concert efforts to achieve tangible results in the field of military applications of 5G that can be shared between NATO and national military communities. Many of the initial reference 5G military scenarios described in this paper deal with NATO and/or national capability development (5G-based private military systems to support operations), interoperability (5G augmentation systems for cost-effective communications interoperability in select scenarios), IT Infrastructure for NATO/national military users, and/or the use of public 5G (civil) telecommunications networks by the military. Combining R&D efforts in this area would achieve critical mass in the effort in a cost-effective approach aligned with Smart Defence concepts.

### Standards Key---2AC

#### Bans alone are insufficient---only standard setting solves.

Bruce Schneier 20, fellow and lecturer at the John F. Kennedy School of Government at Harvard University, 1/20/2020, "China Isn’t the Only Problem With 5G," Foreign Policy, <https://foreignpolicy.com/2020/01/10/5g-china-backdoor-security-problems-united-states-surveillance/>, RMax

The security risks inherent in Chinese-made 5G networking equipment are easy to understand. Because the companies that make the equipment are subservient to the Chinese government, they could be forced to include backdoors in the hardware or software to give Beijing remote access. Eavesdropping is also a risk, although efforts to listen in would almost certainly be detectable. More insidious is the possibility that Beijing could use its access to degrade or disrupt communications services in the event of a larger geopolitical conflict. Since the internet, especially the “internet of things,” is expected to rely heavily on 5G infrastructure, potential Chinese infiltration is a serious national security threat.

But keeping [untrusted companies](https://www.economist.com/china/2019/08/08/huawei-is-trying-to-solve-a-hard-problem) like Huawei out of Western infrastructure [isn’t enough](https://www.nytimes.com/2019/09/25/opinion/huawei-internet-security.html) to secure 5G. Neither is banning Chinese microchips, software, or programmers. Security vulnerabilities in the standards—the protocols and software for 5G—ensure that vulnerabilities will remain, regardless of who provides the hardware and software. These insecurities are a result of market forces that prioritize costs over security and of governments, including the United States, that want to preserve the option of surveillance in 5G networks. If the United States is serious about tackling the national security threats related to an insecure 5G network, it needs to rethink the extent to which it values corporate profits and government espionage over security.

To be sure, there are significant [security improvements](https://www.5gamericas.org/wp-content/uploads/2019/08/5G-Security-White-Paper-07-26-19-FINAL.pdf) in 5G over 4G—in encryption, authentication, integrity protection, privacy, and network availability. But the enhancements aren’t enough.

This design dramatically increases the points vulnerable to attack.

The 5G security problems are threefold. First, the standards are simply too complex to implement securely. This is true for [all software](https://www.schneier.com/essays/archives/1999/11/a_plea_for_simplicit.html), but the 5G protocols offer particular difficulties. Because of how it is designed, the system blurs the wireless portion of the network connecting phones with base stations and the core portion that routes data around the world. Additionally, much of the network is virtualized, meaning that it will rely on software running on dynamically configurable hardware. This design dramatically increases the points vulnerable to attack, as does the expected massive increase in both things connected to the network and the data flying about it.

Second, there’s so much backward compatibility built into the 5G network that older vulnerabilities remain. 5G is an evolution of the decade-old 4G network, and most networks will mix generations. Without the ability to do a clean break from 4G to 5G, it will simply be impossible to improve security in some areas. Attackers may be able to force 5G systems to use more vulnerable 4G protocols, for example, and 5G networks will [inherit](https://gcn.com/articles/2019/10/21/5g-security.aspx) many existing problems.

Third, the 5G standards committees missed many opportunities to improve security. Many of the new security features in 5G are optional, and network operators can choose not to implement them. The same [happened](https://www.wired.com/story/5g-more-secure-4g-except-when-not/) with 4G; operators even ignored security features defined as mandatory in the standard because implementing them was expensive. But even worse, for 5G, development, performance, cost, and time to market were all prioritized over security, which was treated as an afterthought.

Already problems are being discovered. In November 2019, researchers [published](https://techcrunch.com/2019/11/12/5g-flaws-locations-spoof-alerts/) [vulnerabilities](http://www.documentcloud.org/documents/6544575-5GReasoner.html) that allow 5G users to be tracked in real time, be sent fake emergency alerts, or be disconnected from the 5G network altogether. And this wasn’t the first [reporting](https://i.blackhat.com/USA-19/Wednesday/us-19-Shaik-New-Vulnerabilities-In-5G-Networks-wp.pdf) to [find](https://syssec.kaist.ac.kr/pub/2019/kim_sp_2019.pdf) [issues](https://arxiv.org/abs/1806.10360) in 5G protocols and implementations.

## Country PICs

### Country PIC---2AC

#### Unity is key, otherwise disaster ensues.

Lindsay Gorman 19, Fellow at the Alliance for Securing Democracy, 12/3/2019, "NATO Should Count Spending on Secure 5G Towards Its 2% Goals," Defense One, <https://www.defenseone.com/ideas/2019/12/nato-should-count-secure-5g-spending-towards-its-2-goals/161648/>, RMax

Disunity here has real consequences. A split over cybersecurity and the varying presence of “untrusted” suppliers from China in member countries’ 5G networks threatens vital NATO military and intelligence cooperation. The United States has already warned that it will limit intelligence sharing if allies build 5G networks with Chinese equipment. In the words of one official, “the Americans will assume that everything we share with Germany will end up with the Chinese.”

Such an outcome would be disastrous for the alliance. A NATO intelligence-sharing rift would open the door to greater authoritarian interference in Western democracies, and not just from China. NATO’s intelligence sharing and threat analysis cell is a central tenet of its plan to combat hybrid threats from Russia and others: disinformation campaigns, malign financial flows, the annexation of Crimea, and more. Given Russia’s long-standing goal of fracturing NATO, it’s no coincidence that Russian state media champions Huawei.

### Country PIC---1AR

#### Alliance-wide coordination across all-members is key.

Thomas, ’21 (Beryl Thomas, ECFR Alumni, Visiting Fellow at the German Chancellery Fellowship, MA in security policy studies from the Elliott School of International Affairs at The George Washington University, BA in international relations and Italian studies at the University of California, Davis. “What Germany’s new cyber security law means for Huawei, Europe, and NATO” 02/05/21 <https://ecfr.eu/article/what-germanys-new-cyber-security-law-means-for-huawei-europe-and-nato/>) ☺

Berlin’s choice will also have implications for NATO. With Germany seeking to shore up and [encourage America’s recommitment](https://www.spiegel.de/international/germany/germany-s-foreign-minister-on-the-future-of-trans-atlantic-relations-a-68d28367-ae98-4785-bebf-6dbad3990b26) to the organisation, the decisive indecisiveness it has adopted on Huawei is a step backwards in re-engaging with Washington. On 5G, leading NATO members like the US and Germany should be championing efforts to ensure uninterrupted interoperability through bloc-wide standards and minimum network security requirements. This coordination from the outset is necessary because 5G will [give the alliance new opportunities](https://www.defenseone.com/ideas/2020/08/nato-must-move-out-smartly-5g/167687/) for data- and intelligence-sharing as well as allowing it to take advantage of new technologies based on advances in artificial intelligence and machine learning. But with advanced network connectivity comes heightened network vulnerability, and NATO can only realise the full potential of 5G if there is coordination across all member countries.

With this draft law, Berlin has effectively punted down the road a definitive decision on 5G. How the legislation will look in its final form remains to be seen, but Berlin’s preference for Beijing’s tech over Brussels’ wishes is clear. Should the German government fail to take concrete action to block Huawei from its networks, the new law will put Germany at odds with key allies on an issue that has deep implications for security, defence, and the economy.

## DOS CP

### DOD Key---2AC

#### DoD implementation is key – secures operations and ensures military integration

Leleux et al ’21 [Darrin, Deputy Director of the Electromagnetic Spectrum Operations Cross-Functional Team earned his Master of Science in Computer Engineering from the University of Houston at Clear Lake in 1998, and a PhD in Electrical Engineering from Rice University in 2002, Winter 2021, “Fifth Generation Wireless Development in Great Power Competition,” Cyber Defense Review, <https://cyberdefensereview.army.mil/Portals/6/Documents/2021_winter_cdr/02_CDR_Winter_2021_Leleux.pdf?ver=X83q7TOOVMvhrIJHxhBw_A%3D%3D>, St. Mark’s, AM]

The development of fifth generation (5G) wireless technology security is critical for United States (US) national defense and economic security. 5G technology represents a leap forward in the speed and volume of data transmission, as well as a drastic reduction in communication latency, which enables new technologies and operational methodologies. It also has the potential to improve security by interlinking intelligence, surveillance, reconnaissance, and command and control systems by delivering information in real time.[3] The Department of Defense (DoD) must have a strong voice in the development and implementation of 5G technology and associated security measures in order to prevent its adversaries from conducting intellectual property theft, interfering with DoD operations, and compromising the security of DoD personnel, information, equipment, and operational capabilities that will rely on 5G. Since this is a wholeof-nation issue, the U.S. Government (USG) must deliberately incorporate 5G security into conversations with foreign partners, industry, and DoD to evaluate carefully the role of 5G technology in its own, as well as its coalition partners,’ communication architectures and operational capabilities.

#### Winning the tech race requires the DoD – promotes quick response through training and effective tools

Leleux et al ’21 [Darrin, Deputy Director of the Electromagnetic Spectrum Operations Cross-Functional Team earned his Master of Science in Computer Engineering from the University of Houston at Clear Lake in 1998, and a PhD in Electrical Engineering from Rice University in 2002, Winter 2021, “Fifth Generation Wireless Development in Great Power Competition,” Cyber Defense Review, <https://cyberdefensereview.army.mil/Portals/6/Documents/2021_winter_cdr/02_CDR_Winter_2021_Leleux.pdf?ver=X83q7TOOVMvhrIJHxhBw_A%3D%3D>, St. Mark’s, AM]

Recommendation #2 suggests that China will have a great advantage if it is the first to deliver 5G infrastructure and devices globally, gaining first-mover advantage. The DIB reports that “first-mover advantage is particularly pronounced in wireless generation transitions because the leader can set the foundational infrastructure and specifications for all future products.”[30] Many countries will already be beholden to Chinese products when establishing 5G wireless technology networks due to component price and availability of components, as well as compatibility with proprietary interfaces of their current 4G infrastructures or network devices sourced from China.[31] Chinese companies such as Huawei and ZTE Corporation present critical security risks as they are state-owned enterprises linked to the government. This has the potential to create a global information technology (IT) infrastructure susceptible to Chinese predatory practices, such as intellectual property theft and Chinese-mandated technology transfers creating many security vulnerabilities.[32] China’s government has usurped physical and intellectual property, creating an advantage in the information space by exploiting data through creating back door vulnerabilities within hardware and/or software. In 2019, many Chinese IT companies were implicated in nefarious cyber activities and directly linked to China’s government.[33] This linkage can arguably be considered part of the culture as Chinese Law Articles 14 and 17 (National Intelligence Law, enacted June 27, 2017) indicate that Chinese companies have an active role in supplying information and/or access to the state.[34] This culture has provided state-sponsored leverage to make China a peer competitor and adversary of the US, at large, not just DoD. Security Security standards provide the basic parameters to create a secure environment across 5G wireless networks and are vital to maintain the confidentiality, integrity, and availability of US data as it traverses through information networks. To protect US data and systems, several improvements to current systems need to be pursued, including policy changes to ensure only secure equipment is used in USG systems, the development of quantum-resistant cryptography, improvement of software-defined networking technologies, and tighter controls over supply chain management. All these changes must be carefully orchestrated to work in concert with each other across all government agencies and industry partners. Policy and implementation of cryptographic standards are required for global security. US policy protections restrict companies that are non-compliant with current IT security standards from providing equipment for the 5G infrastructure; however, the same standards do not apply to allied countries.[35] These cryptographic standards are being developed by NIST under the U.S. Department of Commerce for use by non-national security federal information systems. Though these systems are for non-national security systems, they could be reviewed or adjusted for applicability to national security systems or critical infrastructure, as well.[36] Smart design of the 5G infrastructure to use these new cryptographic standards would ensure that over the next decade, as the US experience with 5G wireless technology increases and its security is improved, the risk of information theft and unintended decryption remains low. A primary issue is finding a standard that will not impose excessive latency, thereby reducing the benefit of using the new 5G wireless technology. Regardless of the security approaches taken, the US should ensure persistent research and development efforts in security and resilience for the network while operating both in the US and internationally. Resilience Deliberate USG planning and action must be taken to ensure resilience when using 5G wireless systems. Two required actions to ensure a cyber-resilient methodology for US 5G wireless systems are: (1) develop better capabilities to observe anomalies or attacks in real time, and (2) improve the ability for cyber defenders to act at the speed of relevance. USG systems must be able to determine that an attack, malicious event, or exploitation is in progress to take timely actions to ensure system resilience. To identify early warning of an anomaly or attack, US entities must understand their standard day-to-day environment, sense that something is out of the ordinary, and determine what is happening across the digital domain.[37] Additionally, as DoD implements equipment that can leverage the 5G wireless infrastructure, military communications operators need to be trained and have the right tools to detect outside influence. Once an attack is identified, the more difficult task is attributing the activity to a malicious actor and then identifying the attack vector. To accomplish this, DoD should improve training programs for its cyber warriors and develop tools that can detect anomalies and potentially take the first steps in countering cyber-attacks. To help identify attack vectors and determine where an attack came from, new authorities or adjustment to current authorities may be required, especially if autonomous actions are incorporated into these systems. Once a malicious act is identified, military operators must take timely action to stop the event. Finding or identifying the attack vector and stopping the inflow or outflow of data through system manipulation are key. To ensure resilience, military operators should be able to switch between 5G wireless and other secure wireless standards as seamlessly as possible.[38] Regardless of the standards, the key to resilience is having the ability to continue combat operations with or without an available network, albeit with reduced functionality. DoD should continue practicing and exercising scenarios either to maneuver or determine alternate means to remain combat-effective in contested, degraded, or denied electromagnetic spectrum environments. These competitive environments in which the cyber domain is contested are where victory in the next war will most likely be determined.

### DOD Key---Ext

#### Having a clear 5G focus in the DoD is key.

Scharre & Riikonen ’20 [Paul and Ainikki, 11-17-2020, "Defense Technology Strategy," Center for a New American Security, <https://www.cnas.org/publications/reports/defense-technology-strategy>, St. Mark’s, AM]

Technology always has been an integral part of achieving military superiority. A stone axe or wooden club gave a Neolithic fighter a major advantage over an unarmed opponent. As weapons have evolved from bows and arrows to intercontinental ballistic missiles, militaries continuously have sought to harness new technologies to gain an edge on adversaries. Technology alone rarely conveys a decisive advantage, but technology is an enabler for military superiority. When combined with the right organization, training, and concepts for warfighting, technological advantages can make battles hopelessly one-sided affairs. By harnessing advances in stealth, GPS, and precision-guided weapons, the United States dismantled Saddam Hussein’s army during the Persian Gulf War with a 30-to-1 casualty ratio.1 Yet other countries took notice and have been investing in capabilities that have eroded America’s military technological edge.

The United States had a first-mover advantage in the information revolution, but the technology that enabled American military dominance in 1991 now has proliferated. Adversaries have invested in long-range ballistic and cruise missiles that can target American bases and carriers with precision, integrated air defenses to hold stealth aircraft at bay, counter-space weapons to blind military spy satellites and disrupt command-and-control, and cyber weapons to cripple logistics. This suite of capabilities, sometimes lumped under the label “anti-access/area denial,” is meant to hamper America’s ability to project power overseas, buying time for adversaries to change conditions on the ground through force. The United States must transform its way of warfighting to project combat power in the face of these capabilities so the United States can deter and, if necessary, defeat military aggression by potential adversaries.

Senior Defense Department leaders have looked to new technologies, from artificial intelligence (AI) to hypersonic missiles, to reinvigorate the U.S. military’s technological edge vis-à-vis great power competitors. To do so, the United States will need to adopt a technology strategy appropriate for today’s technology landscape. The approach the United States used in the 1960s, ’70s, and ’80s won’t work today, when innovation is increasingly globalized and driven by the private sector. Nor does the U.S. military have sufficient resources to invest in every conceivable technology, even with a $700 billion-plus defense budget. The Department of Defense (DoD) will have to make strategic bets in the technologies most likely to rapidly transform warfare, while hedging against surprise with smaller bets elsewhere.

U.S. defense leaders have sent conflicting signals about their technology priorities. In 2014, then-Secretary of Defense Chuck Hagel launched the Defense Innovation Initiative to develop a “game-changing third ‘offset’ strategy.”2 Then-Deputy Secretary of Defense Robert Work subsequently named AI and autonomy the “technological sauce” to empower this Third Offset Strategy.3 But defense leaders since then have offered shifting and at times conflicting guidance on new technology priorities. Recent Undersecretary of Defense for Research and Engineering (USD(R&E)) Michael Griffin publicly listed his top “priority technology domains” but amended the list approximately four times between its initial release in April 2018 and his departure in July 2020. These priorities fluctuated in number and order; they ranged from 10 to 13 priorities with AI, hypersonics, nuclear modernization, and other technologies rotating up and down in importance. Secretary of Defense Mark Esper remarked at his confirmation hearing that “Different people put different things at number one; [for] me, it is artificial intelligence.”4 Yet the Fiscal Year 2021 Defense Wide Review issued under then-Secretary Esper’s leadership characterized nuclear modernization as “the highest modernization priority.”5 A few months later in April 2020, Director of Defense Research and Engineering for Modernization Mark Lewis stated in an interview, “my number one technology priority is actually microelectronics.”6 With Griffin’s departure, the new Acting USD(R&E) Michael Kratsios identified “microelectronics, 5G, hypersonics, and AI” as technology priorities at his first public event, along with “quantum computing . . . and other industries of the future.”7 In total, five different defense leaders have articulated an ever-shifting array of technology priorities over the last several years with AI, hypersonics, nuclear modernization, and microelectronics all occupying the top spot as the “number one” priority at different times.

DoD leaders’ attempts to publicly communicate their technology priorities are commendable, but the manner in which they recently have done so has been chaotic, confusing, and counterproductive. The DoD needs a coherent technology strategy to equip itself for long-term technology competition. The current approach, in which DoD priorities whipsaw based on the whims of senior leaders, jeopardizes budgetary stability and likely consumes undue time and effort within the department. Esper’s observation that “different people put different things at number one” is precisely the problem.8 Senior leaders are entitled to their views, but a technology strategy that changes every time there is a turnover in leadership creates uncertainty and undermines the department’s ability to make long-term investments.

Rather than a personality-driven approach, the DoD needs a transparent framework for identifying technology priorities that will provide clarity and stability in the department’s priorities. If DoD leaders offer a transparent rationale for which technologies matter, they are more likely to gain necessary support from legislators, the rest of the department, and private industry to achieve technology objectives. Clear priorities are especially critical now, given budgetary competition from the COVID-19 pandemic and the reality that the Pentagon is no longer the primary driver of American technological innovation. The department cannot afford to invest in every technology. To succeed in the long term, it will have to find ways to leverage the evolving innovation landscape and garner the institutional support to do so. The DoD needs a technology strategy to maximize the returns on its technological investments and to signal the rationale behind them.

#### **DoD led 5G security solves.**

DoD 20 – Department of Defense, 5/2/2020, “Department of Defense (DoD) 5G Strategy (U),” <https://www.cto.mil/wp-content/uploads/2020/05/DoD_5G_Strategy_May_2020.pdf>, RMax

Challenge

The ongoing migration to 5G technologies creates multifaceted opportunities and risks. The central challenge for DoD is to accelerate the development and deployment of 5G-enabled capabilities, while ensuring those systems — as well as those of our allies and partners — are robust, protected, resilient, and reliable.

Accelerating the transition to 5G is challenged by key standards, security principles, and spectrum policies that are still in development. Historically, DoD has not engaged with the governance bodies that set mobile wireless industry standards. The international allocation of spectrum for 5G use and the best policies for sharing spectrum among multiple users also continues to be debated. Numerous reviews regarding 5G exports, foreign investment, and technology control measures are still underway. Related factors impacting the cost and speed of 5G deployment include industrial policy, fair market access, and government incentives. Ensuring that DoD can operate in a global 5G environment is challenging because potential U.S. adversaries seek to dominate the 5G market in key partner nations, which could allow such competitors to gain unauthorized network and data access via exploited components in the supply chain, malicious software, and/or insider threats. Given the complexity of 5G infrastructure, even inadvertent vulnerabilities may be very difficult to detect and prevent. Finally, adversaries could leverage control of the 5G market to advance security and foreign policy goals that ultimately undermine U.S. interests.

Because 5G networks will transport massive amounts of sensitive personal, corporate, and government information, they are particularly attractive targets for potential U.S. adversaries. With persistent access to an ally’s 5G network, an adversary could potentially engage in widespread espionage, threaten the privacy and rights of citizens globally, prepare the operational environment to provide an advantage in armed conflict, conduct information operations, and/or disrupt critical infrastructure. For these reasons, 5G networks must incorporate suitable protections. The U.S. Government also encourages allies and partners to prioritize security considerations by avoiding untrusted and unreliable suppliers for their 5G networks, even as DoD seeks to be prepared to operate in all network environments.

Only a robust, in-depth approach to 5G security can address the full range of hardware, software, and human-factor risks, while posturing the DoD to fully leverage 5G-enabled capabilities

#### Security cooperation is key.

DoD 20 – Department of Defense, 5/2/2020, “Department of Defense (DoD) 5G Strategy (U),” <https://www.cto.mil/wp-content/uploads/2020/05/DoD_5G_Strategy_May_2020.pdf>, RMax

International Allies and Partners

DoD must collaborate closely with the State Department to utilize upcoming bilateral and multilateral dialogues to discuss 5G concerns with international partners. DoD must convey to allies and partners the risks to their national security equities — mobilization, interoperability, information sharing, operations, and resilience against coercion — to quickly address them before mitigations become far costlier. The matter is urgent, as many nations are already auctioning 5G spectrum and making long-term investments in 5G infrastructure. It is important that the United States promotes a shared understanding of the importance of 5G protection and the serious threat posed by unauthorized foreign access. The Prague Proposals on 5G security and the National Strategy to Secure 5G provide a helpful basis for framing this issue, specifically noting that "the overall risk of influence on a supplier by a third country should be taken into account".

The decisions made by our allies and partners about 5G deployment often involve senior government and industry leaders who may not view telecommunications infrastructure as a national security issue. DoD must ensure that foreign counterparts understand the risk 5G threats and vulnerabilities pose to interoperability and industrial security so they can accurately communicate the message across their governments. This requires DoD to provide a clear national security-based rationale concerning the risk of 5G vendors beholden to foreign governments.

Some states continue to seek to undermine fair and open international competition for 5G equipment and services via diplomatic pressure, misleading reporting, market manipulations, state-backed financing, and/or other aggressive interventions. The United States is confronting such tactics directly and ensuring that our allies and partners are aware of ties between foreign suppliers and their governments' security organizations. DoD will support these national-level efforts by collaborating with the global community to identify 5G security vulnerabilities and share relevant threat intelligence with DoD counterparts.

In order to influence significant upcoming decisions, DoD must develop clear, prioritized outcomes for international engagement and ensure DoD military, political, and industry outreach is aligned in support of those outcomes. This will include positive messaging about opportunities to collaborate with the United States on 5G research, standards, and deployment.

#### 5G improves military performance

Scott Maucione 22, (Federal News Network Staff, has worked in journalism for over a decade. He previously covered the Pentagon for Inside Defense. 2-1-2022, "5G is changing the way the military connects its bases and its people," Federal News Network, <https://federalnewsnetwork.com/federal-insights/2022/02/federal-insights-smart-base-of-the-future/> ) /billy

As 5G begins to roll out in civilian and military spaces, the Defense Department is testing 5G networks at a handful of bases to ensure connectivity and security.

Since last year, the Pentagon has had contracts for 5G experimentation at nearly a dozen different installations to make “smart bases.”

“In essence, a smart base of the future is the integration of connected technologies that will fundamentally improve the performance and efficiency of assets and services across a military installation,” said Cornelius Brown, Verizon’s Department of Defense sales director, during the Federal Insights discussion Smart Base of the Future, sponsored by Verizon. “As we define smart bases, we can essentially view them as mini cities in itself, where infrastructure, building transportation, energy management, are all factors of a city and a base. What drives a smart base is that they’re all hyper connected, it’s an ecosystem where everything becomes connected.”

That kind of system is what the Pentagon is aiming for when it comes to its future weapons systems, artificial intelligence and how it wants everything to be interconnected with data and interoperability.

“There’s a large collaboration with multiple industry players to really enable various use cases around energy management, drone management, autonomous vehicles, and it’s really a collaborative effort to really prove out what the customer wants to accomplish,” Brown said. “5G brings mobile edge computing closer to the end user, or the application via the cloud. This really removes a lot of historical latency that prevented us from applications being able to make near real time decisions.”

It’s not just the Pentagon’s weapons systems that will see changes with 5G. Military personnel will also see their connected lives move in a different direction as well.

“For military personnel living on the base, they’ll be able to take an autonomous shuttle or bus that will get them around, all that cool stuff,” Bryan Schromsky, a managing partner for 5G public sector at Verizon said. “More importantly they’ll see it in connection. If they’re using a video calling platform on these connected devices, they’ll just have a much better experience. They’ll be in high definition video, they’ll have faster bit rates, so they can do more videos. They can upload information, all of that good stuff and couldn’t ask for much more to have a very intimate and immersive experience in a personal way.”

With that new power and ease also comes new responsibilities and challenges, however.

By adding more devices to the network, it creates more opportunities for malicious actors to get into the network. DoD will need to protect its assets from outside attacks like hackers and inside attacks like a faulty supply chain.

“Having a coordinated security policy is the right approach ,” Schromsky said. “We want to make sure we have a valid, secure supply chain and also work with industry standards. Most importantly we want to have outreach in working with public sector agencies, federal, state and local to make sure that we meet their needs and their challenges.”

DoD will need to rely on future technologies as 5G develops to better security measures.

Schromsky said quantum computing will have a large role to play in encryption and not only making military bases safe, but also securing financial transactions and personal data

### DOD Key---NSA---2AC

#### Interoperability and standardization is key---NSA has authority and expertise

Lauren C. Williams 22 (Senior editor for FCW and Defense Systems, covering defense and cybersecurity. 3-10-2022, "5G has military promise but security concerns are still being untangled," FCW, https://fcw.com/defense/2022/03/5g-has-military-promise-security-concerns-are-still-being-untangled/363003/)/billy

5G offers a number of promising defense applications, particularly when it comes to training on modernized ranges, but security standards still need to be worked out to get the right authorities to operate. Neal Ziring, technical director for the National Security Agency, said that using 5G for military and national security applications requires interoperable and secure standards and policies because they will define how capabilities work together. “In my mind, the critical aspect will not be 5G itself – and that’s going to be important – but understanding how we integrate with it. So if the standards can have security in them, which they’re starting to have…we can ask the carriers from whom we procure commercial service or commercially operated private service [to] turn on those security features,” Ziring said at an AFCEA DC event March 9. “How do we integrate our services, whether it's tactical services or facilities services or training services, to ride over that network in such a way that we know what security guarantees the 5G network itself provides to us and which ones we have to provide as an application service that sits on top?” he asked. Ziring said that would be a crucial question to answer when providing real-time services to a mobile, edge computing environment, which isn’t well standardized yet: “They’re all very virtualized and containerized; that’s an area that’s still a challenge in some quarters for [an authority to operate] at all.” Ziring said the NSA is working with the services and the Defense Information Systems Agency to work out specifications and policy that everyone can use instead of coming up with their own. “We’re looking forward to doing that, but it’s going to be a lot of work over the next two, three years to get to that point,” he said. One of the concepts the NSA is exploring, he said, is the idea of network slicing in which service providers set up independent logical networks across 5G infrastructure, which will be crucial for defense applications of the technology. This means that certain devices (or vehicles) and their authorized users would be designated for a particular network slice with the needed security protections. NSA is working on what the security should be for these slices and the integration risks between cloud and 5G infrastructures. “5G is already being deployed; we’re already having pilots. But I think it’s going to be very important to share security practices and experience as we start rolling these out,” Ziring said. It’s critical that we don’t keep that secret to ourselves, that we share that so we all improve,” he said.

## EU CP

### EU CP---2AC

#### EU policy backfires and only NATO solves.

Agnė Rakštytė 21, Digital Innovation Baltic Fellow with the Transatlantic Leadership team, Chief Operations Officer at the Baltic Institute of Advanced Technology, 2021, “HOW CAN THE BALTIC STATES SUPPORT 5G SECURITY THROUGH TRANSATLANTIC COOPERATION?” *Center for European Policy Analysis*, https://cepa.org/how-can-the-baltic-states-support-5g-security-through-transatlantic-cooperation-08-26-21/, RMax

By late 2020, at least 53 countries had joined the U.S.-led Clean Network initiative, which also was highlighted by the EU as having synergies with its own 5G cybersecurity toolbox, a set of measures adopted to guarantee the security of 5G within EU member states.8 Even though the 5G toolbox addresses the same security issues and specifies strategic tools to mitigate principal cybersecurity risks, it does not set out full unified and detailed regulation for countries within the EU. It simply suggests a general framework and points out where member states could take specific individual measures to protect their 5G networks.

Cooperation between EU member states in the field of security is still insignificant and so national security issues such as 5G security measures have to be resolved at the national level. Countries are under considerable pressure both from internal demand for services and the suppliers themselves to make commitments to specific suppliers and decide who they will be technologically dependent on for the foreseeable future. Because these decisions have to be made at the national level, this has turned individual member states into battlefields for technological influence.

Germany’s hesitation and continued discussions with Huawei about the company’s participation in its 5G rollout raised a lot of concerns, but eventually Germany issued legislation in May allowing the government to block “untrustworthy” suppliers. 9 That same month, Italy approved Vodaphone’s decision to continue its cooperation with Huawei and its participation in the development of its 5G network.10

These events demonstrate that even though most EU countries have taken specific action to secure their 5G networks, we cannot expect to see a unified EU approach to Chinese telecommunication companies anytime soon and this may cause disunity within the EU. However, 5G should not only be considered a national security matter, it must be seen as a grave security issue for NATO. Future military solutions will potentially rely on commercial 5G solutions. The protection of essential networks from the influence of potential adversaries should be a critical strategic goal for NATO.

#### Developing NATO resilience is necessary.

Kadri Kaska 19, head of the Legal Branch and legal researcher at the NATO Cooperative Cyber Defence Centre of Excellence; Henrik Beckvard, researcher at the CCDCOE Strategy Branch; and Tomáš Minárik, researcher at the CCDCOE, 2019, “Huawei, 5G and China as a Security Threat,” *NATO Cooperative Cyber Defence Centre of Excellence*, <https://ccdcoe.org/library/publications/huawei-5g-and-china-as-a-security-threat/>, RMax, Note: ‘of’ was changed to ‘on’ because the authors clearly intended to say ‘on’, change denoted in brackets

The dilemma at hand primarily concerns civilian networks, so it is not overly likely that NATO will take a lead in coordinating action. However, the NATO Alliance is, and will remain, an important venue for allies and partners for sharing information on threats, and that capacity should not be viewed as separate from defining a common approach among liberal (and European in particular) democracies. The issue of Huawei technology is, however, not without relevance to the Alliance. NATO depends of [on] national critical infrastructure to execute national operations and missions. Infrastructure security issues may affect NATO networks or deployed networks such as the Federated Mission Network. Such networks can also be exposed to risk because their extensions may use host nation civilian infrastructure.

### EU CP---1AR

#### NATO role is key---EU alone ignores security risks.

Julia Pallanch and Amy Yanan Zhang 21, Program Assistant of the Asia Program at the German Marshall Fund of the United States. BA degree in Sinology, MA degree in Modern East Asian Studies, her portfolio includes the management of operations concerning the Stockholm China Forum, and the India Trilateral Forum. 10-27-2021, "China, 5G, and NATO Security," GMFUS, https://www.gmfus.org/news/china-5g-and-nato-security)/billy

Strong, modern telecommunications infrastructure capable of intercepting and withstanding hybrid interference is a prerequisite for NATO to deliver on its key mission of collective defense. Yet, this infrastructure in Europe is largely privately owned, and as such is left exposed to the risk of external interference and susceptible to economic decisions that can neglect national security aspects if not clearly regulated by law. Russia is no longer the only state actor resorting to various types of hybrid tactics on NATO territory: China, too, has been using various sophisticated political and non-military tactics to advance its political and economic influence. In the face of these existing threats, it is imperative for NATO and the EU to delineate their scope of action, especially in instances—such as telecommunications—where the line between civil and military infrastructure is not clearly marked.

### EU CP---Parters---1AR

#### NATO key---partner nations are ready for multilateral standards.

Agneska Bloch and James Goldgeier, 2021; Senior Research Assistant, Center on the United States and Europe at The Brookings Institution and professor of International Relations at American University “Finding the right role for NATO in addressing China and climate change” https://www.brookings.edu/wp-content/uploads/2021/10/FP\_20211026\_nato\_china\_climate\_bloch\_goldgeier.pdf//ekc

NATO’s tools for responding to the China challenge

A decade ago, discussions about a forum for NATO conversations on China centered on the idea of a NATO-China Council, analogous to the NATO-Russia Council (NRC), a structured dialogue between the alliance and Moscow initially designed to ease the impact of NATO’s enlargement into Central and Eastern Europe on the West’s relations with Russia.23 But the experience of the NATO-Russia Council demonstrates the limits of such a body; while presumably it should be important as a crisis management mechanism during a major conflict, the NRC failed to perform that role during the 1999 Kosovo war, when Russia suspended its participation in the NRC’s predecessor, the Permanent Joint Council,24 and during the 2008 Russia-Georgia war, when NATO declared it could not “continue with business as usual” in the NRC.25 NATO proceeded to “[suspend] all practical cooperation” with Russia after the latter’s invasion of Ukraine in 2014, despite seeking to keep a channel for dialogue open.26

While a forum for NATO-China discussions could prove useful beyond the military-military staff talks that have been held previously, NATO needs an internal alliance forum to help member states develop greater cohesion in responding to the myriad challenges that Beijing poses, namely in areas like 5G and artificial intelligence.27 In their report, the NATO reflection group suggested forming a “consultative body modeled on the Coordinating Committee for Multilateral Export Controls” that operated during the Cold War.28 CoCom, as it was known, was a voluntary mechanism with no formal enforcement procedures that enabled allied conversations to develop joint policies restricting the exports of sensitive technologies to the Soviet Union, China, and other Eastern bloc nations.29

The Cold War fear of keeping advanced Western technology out of the hands of the Soviet Union was a different challenge than the current concern that Chinese technologies will prove attractive to Western nations, giving Beijing the ability to infiltrate targets and inhibit operations during a crisis. To develop a common assessment of the threat China poses to building common approaches to technology investments within allied nations, the internal NATO forum30 could serve as a platform to support key bodies such as the European Union, which will play a more important role than NATO in European decisionmaking on technology investment.31

NATO countries need to guard against falling prey to China’s divide and conquer strategy facilitated through Beijing’s own institutional mechanisms such as the Belt and Road Initiative32 (BRI) that China has pursued in Europe — primarily through the 16+1/17+1 format that includes countries throughout Central and Eastern Europe — and Beijing’s bilateral economic relations with European countries.33 (In 2019, Italy signed a Memorandum of Understanding to join the BRI, becoming the first G-7 country to do so.34) In one notable example of China’s economic power fracturing cohesion among democratic states, Athens blocked an EU statement criticizing China’s human rights abuses in the United Nations Human Rights Council just months after the state-owned China Ocean Shipping Company bought a 51% stake in Greece’s largest port, Piraeus.35

Coordination on technology investment decisions requires building stronger NATO-EU and U.S.-EU ties. In May 2021, the EU agreed to include Canada, Norway, and the United States in the Permanent Structured Cooperation (PESCO) Military Mobility project, an important sign for future U.S.-EU defense cooperation.36 Building on a European Commission proposal,37 the United States and European Union at their June 2021 summit announced the creation of a U.S.-EU Trade and Technology Council to set joint standards on new technologies, “with the aim of promoting a democratic model of digital governance.”38 This council, which convened for the first time in September 2021, fits into a broader effort by the Commission to set forth an EU-U.S. agenda, creating a common framework for technology governance to ensure “secure 5G infrastructure across the globe and open a dialogue on 6G… part of wider cooperation on digital supply chain security done through objective risk-based assessments.”39 Others have proposed a NATO-EU collaboration to establish an AI Center of Excellence that would more proactively address Chinese advances in artificial intelligence.40

NATO has a ready-made framework for working with Indo-Pacific partners through its global partnership program, which includes Japan, South Korea, Australia, and New Zealand, among other nations.41 Foreign ministers from these four partners met at the North Atlantic Council (NAC) in December 2020 for the first time, and the NAC should hold such meetings on a regular basis to strengthen ties between NATO members and key U.S. democratic allies in Asia. The NATO 2030 expert group has suggested that NATO also seek a future partnership with India.42

Chinese deployments in the Euro-Atlantic area and increasing European (primarily U.K. and French) deployments in the Indo-Pacific will result in greater needs and opportunities for connectivity among U.S. allies across regions. Former U.S. Deputy Assistant Secretary of Defense for Europe and NATO Policy Ian Brzezinski has suggested that NATO could establish a small military headquarters in the Pacific through United States Pacific Command (PACOM) to help coordinate allied deployments in the region.43 One way to begin building more multilateral interoperability in the Indo-Pacific would be to build a defense college for civilian and military leaders in the region similar to the NATO Defense College in Rome.44 Such a college could include not just officers and political staff from America’s Asian allies but could serve to bring Europeans together with their Asian counterparts.

The accelerating importance of the Quadrilateral Security Dialogue or Quad (made up of the Indo-Pacific powers Australia, India, Japan, and the United States), along with formats like the FranceIndia-Australia trilateral forum, creates opportunities for the U.S. and its allies to strengthen ties with India.45 The United States has long worked closely with the U.K., France, and Germany in a NATO Quad on matters of significance for the transAtlantic area. Under U.S. leadership, a Quad plus Quad arrangement could bring key American allies plus one key non-allied security partner, India, together from Europe and the Indo-Pacific, and is a natural outgrowth of the NATO global partnership mechanism. Such conversations would primarily be political in nature, as key allies from these two regions could discuss the growing challenges that China poses. A Quad plus Quad arrangement might also help ease the tensions with France that erupted with the announcement of the AUKUS trilateral security pact and submarine deal between the U.S., U.K., and Australia in September 2021.46

## EU-NATO CP

### EU-NATO CP---2AC

#### NATO should assist the EU with 5G resilience but must coordinate internally first.

Morcos ’21 (Pierre Morcos, visiting fellow with the Europe, Russia, and Eurasia Program at the Center for Strategic and International Studies. “NATO’s Pivot to China: A Challenging Path” 06/08/21 <https://www.csis.org/analysis/natos-pivot-china-challenging-path> ) ☺

Expanding NATO-EU cooperation to help allies build up their resilience in response to China’s growing influence. NATO should step up its cooperation with the European Union when it comes to [screening and assessing Chinese investments](https://www.cnas.org/publications/commentary/enlisting-nato-to-address-the-china-challenge)in allied critical infrastructures, securing 5G telecommunications networks, countering Chinese disinformation campaigns, and spurring joint innovation to maintain NATO’s technological edge in the race against China.

In his [remarks](https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/02/19/remarks-by-president-biden-at-the-2021-virtual-munich-security-conference/)at the Munich Security Conference, President Biden set a clear priority for U.S. allies, saying, “We must prepare together for a long-term strategic competition with China.” If NATO is to play a meaningful role in this collective endeavor, allies must have a better understanding of the security implications of China’s rise, increase political coordination between allies and with NATO’s partners, and enhance cooperation with the European Union.

## Unilateral CP

### Unilateral CP---2AC

#### Transatlantic cooperation is key to 5G cybersecurity and spills over to broader cybersecurity cooperation.

James Lewis 21, Senior Vice President and Director of the Strategic Technologies Program at the Center for Strategic Studies and International Studies; and Clete Johnson, Partner at the Wilkinson Barker Knauer, LLP, 3/1/2021, “Accelerating 5G in the United States: Executive Summary,” <https://www.csis.org/analysis/accelerating-5g-united-states>, RMax

International Partnership Is Key to 5G Security and Competitiveness

The market for telecommunications infrastructure is global and shaped by high capital costs and economies of scale. The United States should work with allies and like-minded countries to promote international norms that enable secure, trusted, and diversified 5G supply chains that will facilitate greater global adoption of 5G and 5G network infrastructures.

Partnership is the key to supply chain trust and to 5G cybersecurity. Developing a common approach to 5G creates opportunity for cooperation on cybersecurity among Western democracies. This common approach could identify common measures to mitigate the main cybersecurity risks of 5G networks, provide advice, and share intelligence on how to do this. One starting point is the European Union’s 2019 Coordinated Risk Assessment on Cybersecurity in 5G Networks, which identified threats and threat actors and vulnerabilities, including vulnerabilities created by the legal and policy frameworks of third countries. In 2020, the European Union endorsed a joint “toolbox” of mitigating measures agreed by EU member states to address 5G security risks. This European initiative, in which the United States was involved, provides a starting point for further collaboration on cybersecurity as 5G technology evolves.

Cooperation in countering predatory practices and in cybersecurity, aligning and coordinating trade promotion policies, and collaboration in protecting standards processes point to the need to work with allies. The basis for renewed cooperation is the shared values of the transatlantic community. These values are now under threat from powerful and ambitious authoritarian regimes, and a growing concern over their behavior offers the United States an opportunity to build a new approach to technological security, including in 5G, with European nations and Asian democracies. The United States should work with allied countries to establish international norms that enable a secure, trusted, and diversified 5G supply chain without creating fragmented or nationalized markets.

5G is a different kind of network architecture. Great reliance on the cloud and pushing processing to the edge offers opportunity for greater security, as does an increasing reliance on a supply chain based on American software and semiconductor technology. Cybersecurity will remain a challenge for the foreseeable future. Our goal with 5G should be that the move to new technology does not increase that challenge and, preferably, would actually shrink it. The emphasis on supply chain security in the last few years has closed off one avenue to potential risk. Further progress will require addressing cybersecurity fundamentals and closer partnerships with like-minded nations.

### Unilateral CP---1AR

#### US action alone is insufficient.

James Lewis 18, Senior Vice President and Director of the Strategic Technologies Program at the Center for Strategic Studies and International Studies, December 2018, “How 5G Will Shape Innovation and Security,” <https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/181206_Lewis_5GPrimer_WEB.pdf>, RMax

A few years ago, no Western company was ready to challenge Huawei and ZTE, but this has changed. Western companies routinely outspend their Chinese competitors in 5G R&D and hold 10 times as many 5G patents. Chinese companies still depend on the Western companies for the most advanced 5G component technologies, such as radio frequency processing or FGPAs (a specialized semiconductor essential for software defined networks).6 The issue is not who leads, but how to maintain that lead.

The United States cannot meet the 5G challenge on its own. When the United States has overcome against Chinese industrial policy in the past, it has been done in concert with U.S. allies. The United States will need a unified approach among like-minded companies and states who are willing to invest in 5G. Part of creating this approach may be to define voluntary agreements on security standards for secure 5G networks.

### Unilateral CP---AT: Private Sector---1AR

#### Military innovation key---dual use tech is more likely to come from military prototypes.

John Breeden 22 (Journalist and reviewer with over 20 years of experience covering technology. He is the CEO of the Tech Writers Bureau. 4-21-2021, "Why the Military Is Leading the Charge on 5G," Nextgov, https://www.nextgov.com/ideas/2021/04/why-military-leading-charge-5g/173438/)/billy

The Military’s Big Plans for 5G

The Department of Defense sees 5G technology as a true game changer for military forces, able to one day turn the tide of battle and give our side an insurmountable edge. It’s not unlike the way that the military heavily invested in radar technology during World War II. The DOD sees 5G as being able to make that kind of difference one day. To that end, they are aggressively pursuing their 5G Strategy Implementation Plan. The plan includes promoting 5G technology development, testing both the advantages and potential vulnerabilities of 5G, engaging with private-sector partners and actively influencing industry as policies and standards are developed and put in place. They are already pushing forward with those plans. Marine Corps Logistics Base Albany, Georgia; Joint Base Lewis-McChord, Washington; Naval Base San Diego, California; Nellis Air Force Base, Nevada; and Hill Air Force Base, Utah, all now have 5G technology testbeds as part of the “Tranche 1” phase of their plan. They are actively testing everything from telemedicine to Battlefield of Things initiatives. And the DOD is gearing up to begin the Tranche 2 phase, which will bring more testbeds online at more bases.

DOD Is Already Testing Prototypes

We are still at the very early stages of 5G, but some of the technology’s potential uses are already gearing up for testing. For example, the Defense Innovation Unit is working with private companies to develop what it calls the Private 5G Program. The idea is that they can design a small unit that can be dropped in almost anywhere and then be activated to provide full 5G networking within a certain geographic area. The Private 5G Program can work regardless of the existing physical infrastructure in the area, so if there are no cell towers, it won’t matter. In fact, it’s being designed to work specifically in areas of low bandwidth, no bandwidth and even areas with potentially contested bandwidth. It could be just as useful to a squad of soldiers operating behind enemy lines on foreign soil as it is to National Guard troops performing search and rescue operations or firefighting in remote areas back home. And the DOD is learning about the pros and cons of 5G through these testbed programs as well. For example, one might think that providing 100 times the bandwidth might make 5G technology less secure because it increases the footprint for attackers. But the opposite is actually true. In fact, 5G has a lot of inherent advantages in terms of security compared with 4G or 802.11 wireless technology. For example, most of the data traffic on a 5G network can be routed thorough the IP tunnel, which is encrypted by default. The DOD can then layer even more security on top of that without worrying about clogging up the bandwidth of a 5G network.

The Biggest Innovations Are Coming Soon

As impressive as the prototypes coming out of the DOD 5G testbeds are today, many of them, like DIU’s Private 5G Program, involve the infrastructure itself. The real innovation will come after the infrastructure is established. Then we will start to see things like artificial intelligence, robotics, predictive analytics, environmental sensing and things we can’t even really imagine yet starting to follow. There are programs that the military wants to do now that simply aren’t possible using a 4G network or 802.11 wireless technology. The testbeds are not only showing how 5G will work, but what is possible once the technology is in place. Who knows what innovations are on the horizon. Will we see autonomous military vehicles, augmented reality-based navigation, real-time 3D imaging of an entire battlefield, or any number of seemingly impossible ideas suddenly becoming feasible? One thing that is almost a certainty is that it will be the military driving the trends this time. Like GPS when it first came out, these new 5G innovations will likely start as military-only tools before slowly making their way to the mainstream. And at the pace that DOD is setting, we can expect to see a lot of really interesting ideas becoming reality very quickly as 5G continues to evolve.

### Unilateral CP---AT: DSS---2AC

#### Can’t solve cybersecurity – reallocation opens up weaknesses for cyber attacks

Alhakami ’14 [Wajdi Alhakami, 2014, “Spectrum Sharing Security and Attacks in CRNs: a Review,” <https://thesai.org/Publications/ViewPaper?Volume=5&Issue=1&Code=IJACSA&SerialNo=11>, St. Mark’s, AM]

However, from a security viewpoint, no spectrum sharing classifications, which are discussed in section 2, are secure against any malicious behaviour while they are not supported with security mechanisms for protection and detection (see table 1). Generally the attackers’ intention is to determinate an effective strategy that exposes a predictable risk. For instance, when CCC is used in the cooperative method of decentralised CRNs for exchanging information about the available channels and the selected channel for data transmission between SUs, it is more prone to various attacks based on selfish and malicious behaviours [41-42]. Because it is regarded as a valuable structure for the attacker to access the channel and gain the most sensitive information, a key approach for some types of attackers involves applying a PUE attack. Moreover, it is more exposed to other attack types such as eavesdropping and DoS, which can be launched easily due to existing weaknesses within the MAC layer, where poor authentication and an existing lack of encryption mechanisms enable an attacker to detect available channels that they can occupy to forge or drop MAC frames, as shown in Figure 7 [41, 56, 90].

### Unilateral CP---AT: DSS---1AR

#### DSS can’t solve – takes years, no tech, and can’t facilitate between systems

Rysavy ’21 [Peter, 4-6-2021, "No magic spectrum sharing solutions," <https://www.fiercewireless.com/regulatory/no-magic-spectrum-sharing-solutions-rysavy>, St. Mark’s, AM]

Together, the FCC plan and the DoD responses demonstrate that dynamic spectrum sharing (as envisioned by DoD) is not a realistic option for widespread 5G commercial networks. The FCC states in its order, “Permitting licensed-by-rule operations would require implementing coordination mechanisms similar to the Spectrum Access Systems found in the Citizens Broadband Radio Service, thereby adding complexity to this band not otherwise required.”

Even for the near future, the DoD RFI responses yielded no magic spectrum sharing solutions. The RFI suggested that DoD is seeking solutions beyond the types of approaches available today, such as CBRS. No response detailed a technology that would facilitate spectrum sharing between different types of systems, such as 5G and military systems. For example, one suggestion was for an enhanced CBRS architecture with a DoD-controlled SAS that operates in near-real-time, but such an approach would take years to develop.

#### US initiatives solve spectrum problems – Europe is looking to use our model

Walko ’21 [John, 9-30-2021, "Europe Struggling to Share Spectrum," EE Times Europe, <https://www.eetimes.eu/europe-struggling-to-share-spectrum/>, St. Mark’s, AM]

The majority may favor the Licensed Shared Access (LSA) route, a technique largely developed in Europe, but there is certainly no unanimity, with some countries preferring a method by which operators would be allowed to share spectrum voluntarily for the fastest services.

“Even though the underlying technologies for many of the potential approaches are well-understood, catering to the many local specifics is proving to be a difficult task,” said Sumanasena. “This is despite the fact that in Europe, as everywhere else, demand for higher speeds and more innovative services is increasing exponentially.”

Sumanasena added that the U.S. is showing the way on what can be achieved, with its focus on developing and then implementing its Citizens Broadband Radio Service (CBRS) after a far-sighted Federal Communications Commission (FCC) gave the all-clear. (It should be noted that CBRS has nothing to do with the CB radio network). “It was a complex business getting from concept to commercialization, taking some seven years, with multi-layer approaches and on whole new technologies,” he said. “But the U.S. is now certainly reaping the rewards.”

### Unilateral CP---Links---Politics---2AC

#### Spectrum sharing gets perceived as nationalizing 5G – it’s controversial with industry, lawmakers, and officials

Gould & Eversden ’20 [Joe and Andrew, 10-22-2020, "Talk of national 5G plan from DoD causes confusion, concern among lawmakers," C4ISRNet, <https://www.c4isrnet.com/battlefield-tech/it-networks/5g/2020/10/22/talk-of-national-5g-plan-from-dod-causes-confusion-concern-among-lawmakers/>, St. Mark’s, AM]

WASHINGTON — Pentagon IT leaders have spent the week insisting the Defense Department does not want to build its own 5G network after a controversial request for information troubled lawmakers, including, most recently, House Armed Services Committee Chairman Adam Smith.

The White House is reportedly pressuring the Pentagon to lease some of its prized spectrum for the lucrative 5G market to a single politically connected company, Rivada, using a non-competitive process. The White House’s push to fast track a contract for mid-band spectrum to Rivada Networks has alarmed senior administration officials, according to CNN.

Rivada and the Pentagon have both rejected those reports, but the denials haven’t squelched concerns on Capitol Hill that the administration is using the Defense Department to make an end-run around regulators in pursuit of an expensive boondoggle.

The concern on Capitol Hill and elsewhere stems from a September RFI from the Department of Defense that seeks industry input on dynamic spectrum sharing, or ways the Defense Department and commercial entities can safely operate on the same spectrum bands.

The RFI asks “how could DoD own and operate 5G networks for its domestic operations?” and “what are the potential issues with DoD owning and operating independent networks for its 5G operations?,” which has fueled fears and pushback in industry about DoD nationalizing a 5G network.

In a statement to C4ISRNET on Wednesday, Pentagon spokesperson Russ Goemaere said “No, DOD does not intend to own and operate a national 5G network.” Rather, he said, the DoD needs to better understand how dynamic spectrum sharing can support training, readiness and lethality in the contiguous United States.

"This RFI will help DOD understand best methods and approaches for owning and operating independent DoD 5G networks supporting ‘spectrum for training, readiness, and lethality,’ " Goemaere said.

Rivada has also denied allegations that it’s in favor of a nationalized 5G network.

“We want to add our voice to those condemning, in the strongest terms, anyone planning to nationalize 5G in America. Whoever they may be. Assuming they exist,” the company said in a statement Oct. 8.

The company also released part of its response to the RFI earlier in the week that listed several reasons the DoD shouldn’t operate a national 5G network, including costs of operations and maintenance, as well as limited coverage and capacity.

Frustration on the Hill

The plan has been met with opposition from the wireless industry, Republican and Democratic lawmakers, and reportedly senior officials within the Trump administration. On Wednesday, Smith told reporters he too is opposed to what he has heard so far.

#### Spectrum sharing links to politics – empirics prove.

Taylor ’19 (Margaret Taylor, senior editor and counsel at Lawfare, fellow in Governance Studies at the Brookings Institution, former Democratic Chief Counsel and Deputy Staff Director for the Senate Foreign Relations Committee (2015-2018). “What Congress Is (And Isn’t) Doing on 5G” 08/28/19 https://www.lawfareblog.com/what-congress-and-isnt-doing-5g) ☺

In theory, government control of the 5G network could increase security and ensure that 5G reaches rural markets where there is currently little profit incentive for private industry to build infrastructure and provide services. Congressional responses to proposals to nationalize parts of the 5G network offer a window into the political aspect of the 5G issue.

The nationalization idea has been advanced twice, each time for a different reason. First, in early 2018, a [leaked National Security Council memo](https://www.axios.com/trump-team-debates-nationalizing-5g-network-f1e92a49-60f2-4e3e-acd4-f3eb03d910ff.html) proposed that the U.S. government pay to build a single 5G network—an unprecedented nationalization of private infrastructure—in order to compete with China and protect the system from malicious cyber actors. Second, in March 2019, Politico [reported](https://www.politico.com/story/2019/03/01/trump-campaign-5g-1230276) that Trump 2020 campaign officials supported a proposal—which reportedly “spark[ed] wireless industry fears of nationalization”—under which the government would take over spectrum designated for 5G and develop a system to share the spectrum with wireless providers on a wholesale basis. According to [Politico](https://www.politico.com/story/2019/03/01/trump-campaign-5g-1230276), this was a bid by Trump campaign officials to woo rural voters who have lacked adequate internet service in the absence of financial incentives for wireless companies to offer affordable broadband. The plan was [reportedly](https://www.fiercewireless.com/5g/confusion-reigns-trump-2020-s-5g-wholesale-vision) backed by Trump 2020 Campaign Manager Brad Parscale and Adviser [Newt Gingrinch](https://www.facebook.com/newtgingrich/videos/newt-live-the-american-5g-failure/2262549377351710/).

Congressional pushback was clear and bipartisan. Sens. Ted Cruz, R-Texas, and Catherine Cortez-Masto, D-Nev., twice introduced the thoroughly named [Eliminate From Regulators Opportunities to Nationalize The Internet in Every Respect (EFRONTIER) Act](https://www.congress.gov/bill/116th-congress/senate-bill/918/text?q=%7B%22search%22%3A%5B%22e+frontier%22%5D%7D&r=2&s=3). It would prohibit the president and federal agencies from constructing, operating, or offering wholesale or retail service on a broadband network “unless a duly enacted Act of Congress signed into law by the President provides the President or the agency … with that authority.” An [identical bipartisan bill](https://www.congress.gov/bill/116th-congress/house-bill/2063/text?q=%7B%22search%22%3A%5B%22e+frontier%22%5D%7D&r=1&s=3) was introduced on the House side. And [another](https://www.congress.gov/bill/116th-congress/senate-bill/893/text?q=%7B%22search%22%3A%5B%225g%22%5D%7D&r=3&s=2) [pair](https://www.congress.gov/bill/116th-congress/house-bill/2881/text?q=%7B%22search%22%3A%5B%225g%22%5D%7D&r=2&s=1) of bipartisan, bicameral bills calling for the Trump administration to produce a strategy report contains an explicit limitation that the report “shall not include a recommendation or a proposal to Federalize 5th or future generations mobile telecommunications systems or infrastructure.” Yet another [bipartisan Senate bill](https://www.congress.gov/bill/116th-congress/senate-bill/1625/text?q=%7B%22search%22%3A%5B%225g%22%5D%7D&r=1&s=1) is broader in scope but includes a statement that it is the policy of the United States that “the Federal Government should … support but not build or operate 5G networks.”

## States CP

### States CP---2AC

#### Federal 5G policies key.

Daniel Gonzales et. al, 2022; senior scientist at RAND (of communications, electronic warfare, cybersecurity, cloud computing, quantum computing, terrorist use of the Internet, and cybersupply chain risk management, examining for policy issues for the DoD and DHS) and a professor at the Pardee RAND Graduate School, PhD in theoretical ohysics from MIT and B.S> in physics from Stanford; “Securing 5G: A Way Forward in the U.S. and China Security Competition” RAND Research Report, ISBN: 978-1-9774-0855-6, https://www.rand.org/pubs/research\_reports/RRA435-4.html//ekc

The Key Elements of a 5G Strategy

The U.S. experience with 4G and the debate over how the country should subsequently pursue 5G raise questions of the role and degree of government involvement, type of government policies, and treatment of foreign vendors in developing the telecommunication infrastructure. Although it was not apparent in the U.S. 4G rollout, the United States must now also consider the role of allies in developing and implementing a 5G strategy and focus more on securing its supply chain.

5G technology, infrastructure, and supporting elements, such as spectrum availability, span across various U.S. government agencies and departments. Any successful strategy to secure 5G will need to account for these different institutions**.** In Table 6.1, we briefly discuss U.S. government departments and agencies with a role in U.S. 5G.

In developing and implementing a strategy to secure the U.S. 5G infrastructure, the government—which includes all the stakeholders listed in Table 6.1—must account for the following key elements: • the role of government funding and investment for R&D • development of secure 3GPP technical standards • federal policies that underpin the 5G infrastructure (spectrum, base stations, etc.) • treatment of foreign 5G infrastructure vendors • supply chain security • role of and coordination with allies.

The role of government funding and investment for R&D refers to how the government can assist U.S. private-sector organizations and U.S. SSOs to support 5G technical standards and technologies and how it can assist U.S. academic institutions and companies in developing advanced wireless communication and networking technologies.

Government R&D will also include resources provided to government R&D organizations, such as NIST and ITS to evaluate important properties of 5G technical standards and NSF for basic research in advanced wireless technologies. As discussed, the government played a minimal role in the R&D for 3G and 4G. As a result, NIST, ITS, and NSF research portfolios in wireless communications have historically been small. Given the security considerations that 5G has amplified in telecommunications, the government has demonstrated an increased emphasis on the development and deployment of 5G.

Thus, the second element, federal policies, will also contribute to how the United States develops 5G and at what pace. Many government bodies, such as the FCC, control electromagnetic spectrum in the United States. The policies these bodies implement will dictate when and how 5G can be deployed (spectrum must be made available in the C-band to realize the full benefits of 5G). Spectrum allocation and bandwidth dictate how far apart base stations will need to be spaced, which will influence the cost to wireless carriers for deploying 5G infrastructure.

Third, the U.S. approach to 5G must consider how it treats foreign 5G infrastructure vendors. For example, the United States will need to determine which companies to exclude or include and how it treats foreign vendors that have been included in an allied country’s 5G infrastructure. The reputation of foreign vendors and their willingness to provide security-related information on their products will be important considerations. Their willingness to share with U.S. government officials the sources of the chipsets used in their products—both who designed them and where they were manufactured—will be increasingly important. Foreign 5G infrastructure vendors should be encouraged, but not required, to use U.S.-designed chips. Just as in automobiles, it might be appropriate to not necessarily impose U.S. content rules on 5G infrastructure components manufactured overseas but to set goals that vendors could strive to achieve. This would also enable U.S. officials to track the use of foreign chipsets in U.S. 5G networks.

Fourth, the U.S. approach should also incorporate measures to secure its 5G supply chain. The United States must monitor the security of its 5G supply chain and ensure that major vendors in the supply chain remain trusted. Doing so involves ensuring that vendors do not become victims of cyber or physical attacks that could interrupt the flow of trustworthy 5G systems or components to end users, U.S. wireless carriers, and those in allied countries. As discussed in Chapter Four, U.S. companies in the 5G supply chain depend on third-party vendors in Asia for state-of-the-art microchips necessary for 5G systems. The U.S. government has recognized this dependence and has initiated legislation to support the construction of leading edge microchip foundries in the United States to ensure trustworthiness.

Last, the United States must consider the role of allies and how they decide to secure their own 5G networks. Allied countries, specifically those where U.S. military installations reside, could affect U.S. communications and either invite or mitigate vulnerabilities.

A U.S. strategy for 5G security must incorporate these elements. As discussed throughout this report, many of these elements have emerged in the transition from 4G to 5G—specifically, concerns about the supply chain and rise of Chinese vendors. The next section outlines several options and explores the merits and downsides of each approach.

## Stop 5G CP

### Stop 5G---2AC

#### No one says yes to bans---even hacks think banning 5G is overkill.

Cassauwers ’19 (Tom Cassauwers, Belgian freelance journalist for media such as BBC, Knack, DataNews, EOS and De Ingenieur. “Is 5G bad for your health? It’s complicated, say researchers" 10/07/19 <https://ec.europa.eu/research-and-innovation/en/horizon-magazine/5g-bad-your-health-its-complicated-say-researchers>) ☺

In September 2017, doctors and scientists launched the 5G Appeal, a petition which calls for the EU to impose a moratorium on 5G rollout, citing imminent health dangers like increased cancer risks, cellular stress and genetic damage. The petition now has more than 250 signatories. In March this year, then Brussels minister of environment Céline Fremault blocked a 5G rollout saying she wouldn’t turn the city’s inhabitants into ‘laboratory mice’. In Bern, Switzerland, a protest in May led some administrative areas to block the construction of 5G antennas.

So how different is 5G and could it impact our health? The reality, experts say, is complex.

‘We have been involved in hundreds of studies about electromagnetic radiation and human health,’ said Professor Niels Kuster, founder and director of the Swiss IT’IS Foundation. He was project coordinator for ARIMMORA, a study into the relation between the electromagnetic radiation emitted by power lines and childhood leukaemia.

Both mobile phones and telecom antennas emit electromagnetic radiation, regardless of what network generation they are used for. They send out non-ionising radiation, which is located at the lower end of the frequency spectrum. Most electrical gear emits this type of radiation, from microwave ovens to power lines.

Non-ionising radiation has completely different health effects from ionising radiation, which is higher up the spectrum and includes X-Rays or nuclear radiation, which have proven harmful effects for human health.

Radiation

Non-ionising radiation can affect us in two ways, according to Prof. Kuster. Just like a microwave oven heats food using non-ionising radiation, telecom gear can do the same to the human body if it emits too much.

‘That's well understood scientifically and there are clear safety guidelines for this,’ he said. The International Commission on Non-Ionizing Radiation Protection (ICNIRP), a global scientific body, for example, has determined a norm for this and continually monitors thermal effects.

We have less of an understanding of the second way in which non-ionising radiation can affect us - how it interferes with us biologically, says Prof. Kuster.

There have been claims that telecom equipment causes cancer and electrohypersensitivity where people experience headaches, nausea or even rashes they believe to be the result of exposure to electromagnetic radiation.

Prof. Kuster says that there is very little clear scientific evidence showing that radiation causes the exhibited symptoms associated with electrohypersensitivity. The World Health Organization noted that double-blind studies have been unable to establish a correlation.

The evidence around cancer is, however, more difficult to interpret. Several large-scale epidemiological studies showed mixed results. The most well-known is probably the 13-country Interphone study from 2000 to 2006 with around 5,000 patients. This tried to find a correlation between mobile phone use and cancer.

It concluded that ‘no increase in risk of glioma or meningioma was observed with use of mobile phones’. For people who used mobile phones more intensively at that time, however, there were ‘suggestions’ of higher glioma rates, but errors and biases could not be ruled out, so no causal relationship could be established.

Some animal or lab-based cell studies have shown certain negative health effects from radiation. This eventually led the International Agency for Research on Cancer (IARC) to classify electromagnetic radiation as ‘possibly carcinogenic to humans.’

This may sound scary but refers largely to uncertainty in the results. Aloe vera leaves, for example, are in the same category. Working at a barber shop is in a higher category, classified as ‘probably carcinogenic to humans’ because of the chemicals hairdressers interact with.

Tracking

Other studies are happening right now, such as COSMOS, which is being carried out in the Netherlands, Sweden, Finland, the UK, Denmark and France.

‘In total we’re tracking 290,000 people across Europe, who we consult every five years,’ said Professor Hans Kromhout, an epidemiologist at Utrecht University in the Netherlands who works on the Dutch chapter of COSMOS.

They use information from mobile phone operators to track consenting participants’ actual phone use, and then relate that to health outcomes. This was necessary as from previous studies, it became clear that participants have difficulties accurately reporting their own phone usage.

‘The data for cancer we don’t have yet,’ said Prof. Kromhout. ‘But we recently released a study for Sweden and Finland, which found an association between frequent phone use and headaches.’ But it unlikely due to radiofrequency electromagnetic fields, he adds.

'It would be good if public institutions invested more in research into these fields.'

Prof. Hans Kromhout, Utrecht University, the Netherlands

This study looked at 21,049 Swedes and 3,120 Finns, and tried correlating phone use with headaches, sinusitis and hearing problems. Participants who called more than 276 minutes per week reported a slightly higher degree of weekly headaches. But it turned out that participants who had 2G-phones (which emit more radiation) did not have a higher degree of headaches than those with 3G-phones (which emit less radiation).

And if a clear association between this kind of radiation and cancer was found, an underlying cause would still be missing since we don’t understand the potential biological effects, according to Prof. Kromhout.

‘We still don’t have a mechanism to explain why the human body would have this reaction,’ said Prof. Kromhout. ‘And without a biological mechanism you cannot have a clear, causal relation, because it could just as well be that something else is causing the cancer.’

Millimetre waves

Ever since we’ve had mobile phones, there have been concerns about their negative health effects. In most areas, the 5G debate is a continuation of all of this, which is logical. The radiation 5G emits will largely be the same as it was for 4G, 3G and 2G before, except for one area: millimetre waves.

These waves are higher up the spectrum than the frequencies we have so far used for mobile telecommunications, although they are still non-ionising radiation.

Millimetre waves are a sub-technology of 5G, which can transfer more information, although for shorter distances. For now, these frequencies aren’t being implemented or even auctioned in Europe, although in the US operators have been using them to build their 5G networks. There has been little research about their health effects.

We know, for example, that they don’t penetrate our skin as much as lower frequency waves, yet that could also mean a different risk assessment, with more attention placed on the skin.

‘I don't claim we need to be concerned about millimetre wave exposure,’ said Prof. Kuster. ‘But it's irresponsible to not have much data and expose large groups of people to these fields. So, there should be more investment into tests about this.’

An argument often used against this sort of research though, is that it’s influenced by the private sector. Telecom companies, according to activists, often fund this research to influence it in their direction. Prof. Kuster accepts private sector funds, and in Sweden, COSMOS is partly funded by a number of mobile phone operators, with a scientific institute acting as a ‘firewall’ between the researchers and the companies.

He says that the results of a study don’t depend on where the money came from but on the quality of the research.

‘It would be good if public institutions invested more in research into these fields,’ said Prof. Kromhout, whose COSMOS study is funded by the Dutch government. ‘That way we can also put to rest doubts about the objectivity of researchers.’

Until now the EU has funded some research on electromagnetic radiation, but currently there is no EU project focusing on the health effects of 5G.

So if we aren’t certain about 5G’s health effects, shouldn’t we just ban it until we are and apply the precautionary principle? Not according to both experts.

‘That would be too much,’ said Prof. Kromhout. ‘We should keep studying and observing this question and be vigilant. But a complete ban would be too much and stop technological innovation. We also haven’t seen a large rise of brain cancer in the last 20 years, even though cell phone use has exploded.’

### Stop 5G---Military AI---2AC

**5G is capable of revolutionizing military capabilities—DOD integration is crucial to increased efficiency**

Rajesh **Uppal, 07/10/2022**; Founder/Director of the International Defense Security & Technology Inc. and US-India Science & Technology Collaboration for Security, Project and Program Manager and Strategist in Satellite, Defense & Aerospace, MTech in Satellite Communications with Distinction from Andhra University; “US Launches 5G Military Strategy and Declares 5G Competition as a “New Arms Race” https://idstch.com/military/us-launches-5g-military-strategy-and-declares-5g-competition-as-a-new-arms-race/

Military requirements enabled by 5G

5G is important to DoD because it offers **higher performance and additional capabilities,** particularly for data driven applications and for machine-to-machine communication. These capabilities will become the foundation for a new networked way of war that brings together sensors and machines that will revolutionize the battlespace and the logistics and support functions behind the front lines**. DoD must have access to a 5G defense industrial base** that **provides trustworthy 5G technologies.**

The military requires High-mobility connectivity. Communications devices must operate while vehicles or soldiers are mobile, even at speeds in excess of 100 mph. Samsung researchers confirmed the world's first data rate of 1.2 Gbps, or 150 MB per second on a vehicle cruising at over 100 km/h. 5G soldiers could **receive real-time streaming video** from aircraft, such as the Predator Drone **flying over a battlefield.**

**Military's growing requirements** to gather, analyze, and share information rapidly; to control an increasing number of automated Intelligence, Surveillance, and Reconnaissance (ISR) assets; to command geographically dispersed and mobile forces to gain access into denied areas; and to "train as we fight" requires that DoD maintain sufficient spectrum access," says DOD's Electromagnetic Spectrum Strategy unveiled in February 2014.

The military requirements for higher data rates for **network-centric capabilities** and the **increasing demand for data transmission** to support **situational awareness** is driving the move to higher RF frequencies (60 GHz, 94 GHz). The push to higher radio frequencies makes available greater bandwidths and reductions in size - both attractive propositions for the military in much the same way as it is attractive to civilian users. DARPA, is working on a project called Mobile Hotspots, which would provide millimetre wave communications to troops in remote areas via drones, giving them access to wireless speeds of around 1 Gb per second.

Many 5G systems are based on the wide spectrum available at mmWave frequencies, essentially 30 GHz and above. The giant investments into mmWave will produce a thriving commercial industry generating passive components, radios, power amps, antennas, and the like. This will result in drop in prices of these components, much to the benefit of existing military applications including satellite communication.

Similarly the considerable investment into 5G low-cost phased array antennas, beamforming algorithms, and phase and amplitude adjustable components will lead to cost and productivity advancements for its higher end military phased-array radars. 5G mobile applications will add real-time tracking as well.

Military is interested in deploying 5G wireless mesh networks for its communication needs, which are more robust and self-healing, the communications packets find the best route to the destination based on traffic levels and available system bandwidth. 5G, shall enable mesh networking to enable devices to communicate with each other directly rather than via base stations, which should increase the bandwidth, lower power consumption, reduce infrastructure costs, and improve spectral efficiency.

Military engagements are often spontaneous, and a communications solution needs to be, as well. The communication system should be deployable with little or no fixed architecture. 5G shall enable future

Military Adhoc sensor networks that are expected to be widely deployed for battlefield surveillance, detecting and characterizing Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) attacks and materials.

Each node may be equipped with a variety of sensors, such as acoustic, seismic, infrared, still/motion video camera, etc. These WSNs may connect to the rest of the world through the 5G cellular network. The Mobile phones may themselves be integrated with more and more actual sensor capabilities and form a wireless sensor network.

# Disadvantages

## Eurasia DA

### Eurasia DA---UQ---2AC

#### Euro-Sino relations are in the dumps.

Ian Johnson 22, Stephen A. Schwarzman Senior Fellow for China Studies at the Council on Foreign Relations, 6/10/2022, "Has China Lost Europe?," Foreign Affairs, <https://www.foreignaffairs.com/articles/china/2022-06-10/has-china-lost-europe>, RMax, edited for errors

In April and May, as Russia’s war in Ukraine entered its third month, China sent a special envoy to meet with officials in eight central and eastern European countries. The timing was not coincidental: in the two months since Russia had launched its invasion, China’s standing in Europe had sunk to new lows. European governments were dismayed by Beijing’s strengthened ties to Moscow and its tacit support for Russia’s aggression, and the Chinese leadership hoped to do damage control in a part of the continent where it believed it had special sway.

For a decade now, China has made the countries of central and eastern Europe one of its diplomatic focal points. Offering top-level access in Beijing and dangling huge trade opportunities, Chinese officials believed they could use this belt of smaller, post-communist governments as a counterweight to critical voices in the European Union and U.S. influence on the European continent. And with the war in Ukraine bringing a chill over China’s European relations, Beijing assumed that a series of brisk meetings in the region—including in Budapest, Prague, Riga, and Warsaw—would help turn the tables it [in] its favor. But these efforts went nowhere. Instead, the Chinese ambassador and the rest of her delegation were rebuffed, with the Czech foreign ministry, for example, saying it used the meeting to express “reservations to current Chinese cooperation with Russia.”

Of the many important ripple effects of the war in Ukraine, the growing rupture between China and Europe is perhaps the least appreciated. In earlier years, the Chinese government viewed the European Union as an area of the world where it could pursue its economic interests with fewer of the geopolitical tensions that characterize its relations with Washington. And it set out to use what it saw as its special ties with a large group of countries in central and eastern Europe, in particular, to cement this business-over-politics approach. For European governments that, like China, had transitioned to capitalism in recent decades, China was a powerful new partner that held out the potential of large-scale investment in their economies. In return, Beijing hoped to find a backdoor to Europe’s vast markets, as well as gain new political leverage in its growing rivalry with the United States.

Today, however, Europe has become one of China’s biggest foreign-policy headaches. In part, the current situation is a result of economic miscalculations by both sides, which overestimated the potential benefits of the arrangement. But China’s increasingly rigid position on Taiwan has made things worse. The Chinese government has retaliated against Lithuania for giving a small amount of symbolic recognition to Taiwan; and over the past year, it has made threatening noises toward other European governments over the same issue. Amid these souring relations, China’s support for Russia in Ukraine has brought its European troubles to a head.

The stakes are not small. The war in Ukraine has exposed how few allies China has and how badly the Chinese leadership miscalculated in pursuing close ties with Russia. Beijing’s heavy-handed efforts to gain leverage in Europe have also backfired. Even as its economy and growing military strength guarantee it power and attention, its failed European project has underscored its inability to win durable partners among the advanced democracies—a pattern that seems likely to hinder its long-term influence in the world.

### Eurasia DA---UQ---2AC

#### Decline in relations is inevitable.

Francesca Ghiretti 22, 6-10-22, EU-China analyst, PhD in IR, https://merics.org/en/merics-briefs/china-still-trying-win-eu-over-germanys-shifting-china-relations-taiwan//tyei

While the future direction of EU-China relations seems at least in question, China is prioritizing other partners.

The Regional Comprehensive Economic Partnership (RCEP) and the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) are alternative markets evolving, which will compete with the EU’s single market. China is a member of the former and has applied to the latter.

Beijing is increasingly focusing on the Global South. Following the launch of the Global Security Initiative, China is changing gear in its foreign policy endeavors, bringing forward a more military-focused foreign policy. Despite not going as well as Beijing would have intended, Foreign Minister Wang Yi’s recent Pacific tour is a perfect example of China’s new approach to foreign policy.

The change in gear in foreign policy is in line with China’s long-standing conviction of the West’s historical decline. And in the so-called West, the EU is viewed by China’s leaders as an odd actor, one whose difficulty in balancing national and regional interests and varying competencies leave it unable to advance a credible and effective foreign policy.

### Eurasia DA---UQ---Thumpers---2AC

#### Ukraine, COVID, and economic disputes thump.

Paul Haenle 22, Maurice R. Greenberg Director’s Chair at the Carnegie Endowment for International Peace, visiting senior research fellow at the East Asian Institute; interviewing Philippe Le Corre, nonresident senior fellow in the Europe Program at the Carnegie Endowment for International Peace, 5/10/2022, "Russia’s Invasion of Ukraine Has Jeopardized the China-EU Relationship," Carnegie Endowment for International Peace, <https://carnegieendowment.org/2022/05/10/russia-s-invasion-of-ukraine-has-jeopardized-china-eu-relationship-pub-87107>, RMax

Paul Haenle: How do you think the Ukraine issue will impact the broader EU-China relationship over the long run?

Philippe Le Corre: I think it’s impacting the relationship tremendously. All my contact with Chinese colleagues over the past few weeks . . . it’s been a dialogue of the deaf, in the sense that people don’t seem to realize in China how dreadful this war has been. . . .

There are many issues that the EU is willing to discuss with China. I don’t think the door is closed. There will be more meetings. Their relationship is not as bad as the U.S.-China relationship.

On the economic front, there are many things going on, but there’s also the COVID [pandemic] issue. A number of European countries are not very satisfied with the way China has handled the pandemic for the past year, with many expats not being able to go back and things like the current lockdown.

Also, on the [Comprehensive Agreement on Investment](https://ec.europa.eu/commission/presscorner/detail/es/ip_20_2542) (CAI) [a proposed China-EU investment deal], there was some progress being made through this agreement, which was discussed for seven years—a very long time for an agreement, even by EU standards. The problem is that the EU has to stand for its values and principles. It has a principled diplomacy, as [High Representative of the EU for Foreign Affairs and Security Policy] Josep Borrell [wrote](https://www.eeas.europa.eu/eeas/china%E2%80%99s-choices-and-responsibilities_en) recently. And in fact, members of the EU Parliament are the ones ratifying international agreements, including the CAI. So as long as the members are being [sanctioned](https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2021)690617) by China, it’s going to be very difficult to ratify the CAI at least for the next two years.

We should be continuing to talk about climate, biodiversity, and how to prevent the next pandemic, but on the economic front, it’s not so clear how we’re going to get out of this.

Meanwhile, the relationship is not as smooth as it was before, in terms of Chinese investment in Europe or European investment in China. What’s working well is trade, with a huge deficit in China’s favor.

### Eurasia DA---UQ---Thumpers---1AR

#### Human rights, Taiwan, and Czech disputes thump

Francesca Ghiretti 22, 6-10-22, EU-China analyst, PhD in IR, https://merics.org/en/merics-briefs/china-still-trying-win-eu-over-germanys-shifting-china-relations-taiwan//tyei

Although the Commission remains measured in its approach, human rights and Taiwan have come to occupy an increasingly outspoken role in the EU’s agenda, and the European Parliament is driving it. Following the publication of the “Xinjiang Police Files”, political groups in the European Parliament have pushed a resolution on Xinjiang (more on this in the Buzzword).

During the annual EU-Taiwan trade and investment dialogue, the two have looked to upgrade their economic relationship. China has warned the EU of the risks but has not “punished” the block, not only because the Commission made sure not to cross the political red line, but also because unlike punishing single member states, punishing the whole of the EU may result in shooting oneself in the foot (more on this in the Review section).

The most important change is perhaps occurring in member states who no longer ignore or sideline difficult matters in their dealings with China. Even Germany seems to have taken tangible steps towards curbing its business links with the region. The government has refused to extend investment guarantees for certain Volkswagen projects in China.

However, CEE countries remain the most outspoken and active voices in the debate. The Czech Parliament’s foreign affairs committee has approved unanimously a resolution to leave the 16+1, which is now with the Foreign Ministry. While from July 1, the Presidency of the Council of the European Union will be in the hands of a China-skeptic Czechia, a position aided and abetted by Beijing’s position on Russia’s invasion of Ukraine. The expectation is thus for the China-related agenda of the incoming Presidency to be pushing for a further distancing of the EU from China, which is set to test EU-China relations.

### Eurasia DA---UQ---Economy---1AR

#### Economic policies thump.

Ian Johnson 22, Stephen A. Schwarzman Senior Fellow for China Studies at the Council on Foreign Relations, 6/10/2022, "Has China Lost Europe?," Foreign Affairs, <https://www.foreignaffairs.com/articles/china/2022-06-10/has-china-lost-europe>, RMax

BROKEN PROMISES?

According to Chinese figures, trade between China and its European partners grew eight percent a year between 2012 and 2020 and surged even more during the pandemic. But the growth was starting from a very low base, and the results have been extremely modest. According to the Czech researcher Richard Q. Turcsanyi, China still accounts for less than two percent of the central and eastern European region’s exports and nine percent of its imports; Chinese foreign direct investment has had an even smaller impact, making up less than one percent of total foreign direct investment. That, Turcsanyi has observed, means that central and eastern Europe “has the least Chinese presence when compared to any other region in the world when measured by its shares of economic interaction.” Given Beijing’s decade-long effort to cultivate the region, this is an astonishingly poor showing.

One reason the results were so dismal is that the Chinese approach left it up to Chinese companies to do the actual investing. Although many Chinese companies are state owned, they are still profit oriented. And for these enterprises, central and eastern Europe simply isn’t very attractive. Compared to western Europe, it is less densely populated, cities are dispersed across a large area, there is less infrastructure, and standards of living are lower. No wonder, despite Beijing’s rhetorical encouragement, few Chinese companies have taken up the call to invest in the region.

Seen broadly, China’s mishaps in Europe reflect an approach to policymaking that make sense in the Chinese context but does not always play well overseas, especially in advanced democracies, where governments are more directly accountable to their electorates. Many initiatives in China are often showy affairs that start with a bang and report creatively produced statistics. They offer a statement of intent rather than concrete plans. Content is added later, sometimes years later, or never at all.

Another problem was China’s mercantilist approach to foreign policy and trade—basing foreign relations on calculations of economic gain. All countries do this to some extent, but China is unusual among major powers in relying so heavily on economic ties to shape its foreign relations. Meanwhile, the projects that China has announced have often turned into boondoggles or dead ends. Along with the high-speed rail project, these include a $15.6 billion expansion of the Cernavoda Nuclear Power Plant in Romania, for which the promised Chinese investment never materialized. In 2020, seven years after China had signed on to the deal, the project was taken over by a U.S. consortium. Partly because of the nuclear plant debacle, the Romanian government last year banned Chinese companies from participating in public infrastructure tenders. Other governments in the region have made similar moves, viewing Chinese bidding on contracts as harmful to their efforts to compete with more advanced industrial economies.

### Eurasia DA---UQ---Taiwan---1AR

#### Taiwan policies thump.

Ian Johnson 22, Stephen A. Schwarzman Senior Fellow for China Studies at the Council on Foreign Relations, 6/10/2022, "Has China Lost Europe?," Foreign Affairs, <https://www.foreignaffairs.com/articles/china/2022-06-10/has-china-lost-europe>, RMax

ARM-TWISTING ON TAIWAN

But China’s eroding support in Europe has not been limited to economic failures. Many European governments have increasingly bridled at Beijing’s efforts to use its economic might to silence criticism of its own policies and human rights record. Nowhere has this coercive strategy been more pronounced than on the matter of Taiwan.

Consider the case of Lithuania. In deference to China, most countries in Europe and elsewhere have used the word “Taipei” to describe any Taiwanese representative offices in their countries, the idea being that it was acceptable to use the island’s capital rather than its proper name because the latter somehow implied statehood. When Lithuania decided to flout this convention last year—allowing Taiwan to open a representative office that featured “Taiwan” in its name—Beijing responded with a total economic ban on the country. It not only cut off Lithuanian exports to China but threatened to ban any product manufactured in another country if the item contained a Lithuanian component.

At first, it seemed that Lithuania would find few supporters in Europe for refusing to bow to Chinese demands. That was especially true after China threatened to sanction international companies that used components made in Lithuania. Some EU countries— including Germany, which has a large trade with China—put informal pressure on Lithuania to back down on its pro-Taiwanese stance. Gradually, however, European leaders found Beijing’s hardline behavior intolerable. In January 2022, Brussels launched a case with the World Trade Organization, accusing Beijing of engaging in discriminatory practices because it stopped clearing Lithuanian goods through customs and rejected import applications from Lithuania. It was amid these deteriorating relations that the war in Ukraine turned many European governments more decisively against China.

### Eurasia DA---UQ---Ukraine---1AR

#### Ukraine invasion thumps.

Ian Johnson 22, Stephen A. Schwarzman Senior Fellow for China Studies at the Council on Foreign Relations, 6/10/2022, "Has China Lost Europe?," Foreign Affairs, <https://www.foreignaffairs.com/articles/china/2022-06-10/has-china-lost-europe>, RMax

RUSSIA OVER EUROPE?

The Chinese government’s support for Russia in the lead-up to the invasion caught many European leaders by surprise. Just before the war began, China and Russia issued a joint communiqué that endorsed Russia’s call for NATO to be rolled back to 1997 borders. This action would have stripped countries such as the Czech Republic, Poland, Slovakia, and the Baltic states—all of them members of the 16+1 group that China was supposedly supporting—of NATO weapons and troops, leaving them as vulnerable as Ukraine.

Beijing’s behavior since the war began—repeating the Russian talking point that the invasion was provoked by NATO enlargement—has crystalized the growing unease in European capitals. In March, German Foreign Minister Annalena Baerbock said that the war showed that “one-sided economic alignments in fact make us vulnerable. Not just with regard to Russia.” European frustration with China boiled over after a summit in early April between senior Chinese leaders and the European Parliament. The EU’s top representative for foreign affairs, Joseph Borrell, called it a “dialogue of the deaf.” These sentiments have been especially strong among the members of the 16+1, many of which are now on the frontlines of the face-off with Russia and have themselves benefited from NATO security guarantees.

Several European countries have now openly embraced Lithuania’s outspoken position on Taiwan. One is the Czech Republic, which is also one of the wealthiest countries in the region. In April, Czech Foreign Minister Jan Lipavsky demanded greater scrutiny of China’s support for Russia, accused China of having “bullied” Taiwan, and called for closer Czech-Taiwan relations. Latvia, Lithuania’s close neighbor, has meanwhile called on Beijing to “use more leverage in order to stop Russia’s aggression against Ukraine.”

Notably, the 16+1 itself has seemed increasingly moribund. Last year, six member countries decided against having their heads of state attend a virtual summit with Xi Jinping, sending lower-level officials instead. This year, the 16+1 summit did not take place, possibly because of the war in Ukraine.

#### Ukraine thumps – trade is down and the EU won’t budge

Philippe Le Corre 22, 5-17-22 Former research associate with the Ash Center from 2019-2021, former fellow with the Mossavar-Rahmani Center for Business and Government (M-RCBG) from 2017-2019, sr. fellow in the Asia and Europe programs at the Carnegie Endowment for International Peace and an Associate in Research at John. K. Fairbank for Chinese Studies at Harvard, https://ash.harvard.edu/ukraine-wars-impact-sino-european-relations//tyei

Two months later, on April 1, President Xi held another summit — this time with European Commission President Ursula von der Leyen and European Council President Charles Michel. For the first time in several years, the Chinese leadership faced a stern European side, unwilling to address topics other than the war in Ukraine. Under such circumstances, “there cannot be business as usual,” von der Leyen said. Although China’s ability to influence Putin is limited, the EU still argued that China has unique channels with Russia.

The Chinese side, however, has a very different view. President Xi has called on Europe to have an “autonomous” view of China (presumably autonomous from the United States), and Beijing insists that the solution to the conflict is to accommodate the “reasonable security concerns of all parties concerned.” Still, China has not, by and large, tried to circumvent Western economic sanctions toward Russia — although it is quietly encouraging a coalition of nations who do not want to take sides on Ukraine.

Beijing certainly does not welcome instability and economic turmoil, but China’s image has already dropped significantly in Europe. Since 2020, COVID-19 and the way some Chinese diplomats engaged in propaganda over “mask diplomacy” (through social media and embassy websites) have left scars. Furthermore, Beijing’s willingness to embrace and magnify EU divisions in the early stages of the pandemic has led to a backlash both in European public opinion and governmental elites, who have become irritated by China’s aggressive discourse. This explains the relative hardening of Brussels’ position vis-à-vis Chinese investments, state subsidies, and “coercive economic measures” on a member-state like Lithuania, which was sanctioned by China last year for opening a new Taiwan office. The EU has reacted by launching a case before WTO, calling such actions “discriminatory.”

On a macro-economic level, Chinese foreign direct investments (FDI) have dropped significantly according to a recent MERICS/Rhodium Group report. Although Chinese FDI in Europe increased 33% to $11.1 billion (from $8.3 billion in 2020), 2021 was the second-lowest year (above only 2020) for China’s investment in Europe since 2013. In trade, China was the third-largest partner for EU exports of goods (10.2%) in 2021 and the largest partner for EU imports of goods (22.4%). Following the sanctions on Lithuania, the war in Ukraine, and lockdowns in China, the 2022 picture appears uncertain.

### Eurasia DA---AT: EU Leadership---2AC

#### Alt causes to EU leadership.

Tony **Barber 19**, Europe editor at the Financial Times, 11-4-2019, "New EU leadership team must up its game on foreign policy," https://www.ft.com/content/e08b101e-fa48-11e9-a354-36acbbb0d9b6  
  
The new EU leadership team taking office in Brussels knows that, if the bloc’s common foreign policy is to command respect, the first place where it must achieve success is in Europe’s neighbourhood. It needs to be well-planned, as united as possible, efficiently executed and imbued with a larger sense of long-term strategy. In all these regards, two recent episodes — one concerning the Balkans, and the other Syria — have been little short of a debacle.

Each incident points to the EU’s inability to translate its undoubted weight as a commercial and regulatory bloc into hard power on the world stage. It is not just a matter of lack of military muscle, important though that is. The real problem is that, whenever two or more of the EU’s biggest countries are in disagreement, a common European foreign policy is either ~~paralysed~~ [stagnated] or becomes a question of finding the lowest common denominator among 28 states. An often overlooked point is that these disagreements tend to arise out of domestic political tensions in individual countries — over, for example, irregular migration or attitudes to Islam or Russia. Such tensions hobble the attempts of governments to find common ground with their EU partners.

In any case, France, Germany and other EU countries usually prefer to keep their freedom of manoeuvre when it suits them. The Syrian episode centres on Annegret Kramp-Karrenbauer, who is Angela Merkel’s preferred candidate to succeed her as German chancellor. Ms Kramp-Karrenbauer was named defence minister in July in an apparent attempt to raise her profile with German voters. But the proposal for a multinational security zone in northern Syria that she came up with this month was startling for its naivety and lack of preparation. Before unveiling her plan, Ms Kramp-Karrenbauer, who replaced Ms Merkel as the Christian Democratic party’s leader in December ahead of elections due in 2021, consulted neither her Social Democratic coalition partners nor Germany’s Nato and EU allies. Her proposal skipped over crucial questions such as whether the UN Security Council would endorse it, whether the US would take part and whether Germany’s under-resourced armed forces would send soldiers to Syria. To each question it rapidly became clear that the answer was almost certain to be no. Indeed, it was hard to tell who was more dismissive of the initiative — Russia and Turkey, which control events on the ground in Syria, or Heiko Maas, Germany’s foreign minister, who is of course a colleague of Ms Kramp-Karrenbauer. In this way, the plan served no purpose other than to illustrate the incoherence of the German coalition’s foreign policy, not to mention the EU’s near-irrelevance in Syria.

This is a sobering thought in view of the fact that the 2015 arrival of large numbers of war refugees from Syria and other conflict zones, plus other migrants, precipitated one of the EU’s worst crises since the 1957 Treaty of Rome that set up the bloc.

The EU’s mis-steps in the Balkans are no less painful to watch, but in this case the main culprit is France, not Germany. By blocking Albania and North Macedonia from opening EU membership talks, President Emmanuel Macron shocked and undermined a region whose stability is integral to the stability of the European continent. In North Macedonia’s case, Mr Macron’s move made the EU reek of hypocrisy. For the EU had long promised to start entry talks, provided that the Macedonians compromise with Greece over their country’s disputed name — a condition fulfilled in the Prespa agreement, which came into force last February.

In fairness to Mr Macron, he is not alone in having doubts about enlarging the EU into south-eastern Europe. Denmark and the Netherlands joined France in opposing Albania’s entry talks. Moreover, when the European parliament adopted a resolution last week in favour of starting accession talks with the two Balkan states, some 136 MEPs — or almost a quarter of those who voted — backed Mr Macron’s position. Furthermore, Mr Macron has a point when he suggests that the EU should focus on internal reforms before absorbing new members. The EU’s most important project, the 19-nation eurozone, remains a half-built house. Effective EU-wide action is woefully lacking in areas such as migration and asylum policy. However, Mr Macron would sound more persuasive, but for the persistent rumours that France’s true objective is to close the EU door forever to western Balkan countries. Instead they would be fobbed off with membership of the European Economic Area, which would keep them out of the EU’s political institutions and make them permanent second-class Europeans. The Syrian and Balkan embarrassments are symptoms of an EU unsure of its place in the world and suffering from ineffective Franco-German co-operation. But if the EU cannot get things right on its own doorstep, where can it?

### Eurasia DA---AT: EU Leadership---1AR

#### Collective action problem

Wolfgang **MüNchau 19**, associate editor of the Financial Times, 10-27-2019, "Europe needs to solve its collective action problem," https://www.ft.com/content/0d5126aa-f72a-11e9-9ef3-eca8fc8f2d65

The news is less dramatic than Turkey’s invasion of northern Syria, or our daily fix of Brexit news. But it is hard to overestimate the importance of German chancellor Angela Merkel’s decision to allow Huawei, the Chinese telecoms group, to bid for Germany’s 5G mobile network.

This is the quintessential instance of EU’s collective action problem: a large European country makes a unilateral decision to the detriment of other member states of the bloc.

Germany’s constitutional balanced budget rule is another example. I would classify it as the single most stupid economic policy decision taken by a G7 country in my lifetime. It artificially constrains the ability of fiscal policy to stabilise the economy at a time when monetary policy has hit the limits. The governance of the eurozone is the grandfather of the EU’s collective action problems. Huawei is the grandchild.

The issues with Huawei’s 5G bid will become clear much sooner: the company exposes the EU to security risks. Unless the German parliament manages to overturn Ms Merkel’s decision, other countries are bound to follow. This in turn will limit the EU’s ability to develop an industrial policy towards China. It would be a diplomatic own goal on a scale similar to US President Donald Trump’s decision to pull American troops out of Syria.

There are technical and commercial reasons for Germany to favour the Huawei bid. German telecom operators are already invested in Huawei’s technology. And the German economy would take a hit if China were to respond to a Huawei ban in kind. But these economic effects are small compared to the wider implications. Two of the world’s three 5G producers, Nokia and Ericsson, are European. Why not let European companies build the EU’s 5G network?

As a Chinese company, Huawei would struggle to dispel doubts about its ability to shield sensitive EU data from the Chinese security services.

The EU cannot base its industrial strategy on the illusory hope that a Chinese-owned company might stand up to Chinese politicians or defy Chinese law. 5G is not simply another telephone network. It will be a critical component of the telecommunications infrastructure on which much of our future commercial activity will be based.

By its nature, the EU is not well equipped to deal with this type of problem. It is good at triangulating between the divergent interests of its members, but not at developing a coherent geopolitical strategy. For example, the EU has failed to leverage the euro into a foreign policy tool. Foreign policy was not on member states’ minds when they created monetary union. And despite some minor reforms here and there, the eurozone’s governance framework is still similar to what it was 20 years ago.

A small-country mindset doesn’t simply disappear when states come together to form a union. And today’s policy debate in the eurozone is still full of single-country obsessions like competitiveness and fiscal rules. A similar mindset afflicts foreign policy. In contrast to the Americans, Chinese or Russians, Europeans are framing foreign policy in terms of relationships, not interests. Interest-based policies are discretionary by definition. But the EU is rules-based. As central bankers are only too well aware, rules and discretion do not happily coexist.

The EU has shown that it can act forcefully when there is near-unanimity, as was the case when national leaders responded to Russia’s annexation of Crimea. But that was an exception. More typical has been the failure to agree a joint immigration policy. Immigration is a classic collective action problem where interests are not aligned.

#### Poor leadership and beauracracy.

Prince Michael **Liechtenstein 19**, founder and Chairman of Geopolitical Intelligence Services AG Vaduz, 11-04-2019, "Bureaucracy and centralization are limiting freedom in Europe," https://www.gisreportsonline.com/how-to-destroy-the-european-union,3019,c.html

Expanding bureaucracies

However, Parkinson’s law – that work expands to fill the time available for its completion – took hold in European bureaucracy, which overran institutions. Its growth did not stop at the national level, but infiltrated EU administration. More and more [centralization](https://www.gisreportsonline.com/the-ever-ambiguous-european-union-project,politics,2906.html) and harmonization were imposed through a web of new rules and regulations. Local, national and regional specificities and needs are frequently ignored. This took place even as national bureaucracies grew increasingly excessive. Now, two nannies domineer over European citizens: their national governments and the European Commission.

This situation might still be accepted if Brussels, with the support of some governments, did not harmonize and unify various measures, undermining the principles of self-determination, local control and subsidiarity to the point where individual citizens feel it acutely.

The problem of potentially excessive centralization is a consequence of weak leadership and expedient policies

Although Brexit was initially a result of weak leadership in London, it should serve as a warning against both an “ever closer union” and a “union of different speeds.” [Centralization was the cause](https://www.gisreportsonline.com/shortsightedness-and-stubbornness-are-holding-europe-back,2646,c.html) of the outcome of the Brexit referendum. The problem of potentially [excessive centralization](https://www.gisreportsonline.com/the-eus-tilt-toward-centralization,2414,c.html) is a consequence of weak leadership and expedient policies in member states, which allows for excessive rules, regulation and centralized power.

Discriminating measures

A few years ago, Europe’s central authorities (a majority in the European Council) decided to allocate migrants among member states, often against those countries’ wishes. “Solidarity” was the pretext. The Czech Republic, Hungary and Poland objected and refused to take in those migrants. Last week the Advocate General, an advisory body to the European Court of Justice (ECJ), issued an opinion that the three countries can be fined and forced to accept the arbitrary quota. The ECJ is not obliged to follow the Advocate General’s opinions, but usually does. Interfering in the population policy of individual member states will undoubtedly be perceived as crossing a red line. A ruling is expected early next year.

Again, the problem is one of weak leadership. Since at least the 1990s, it had been evident that a wave of migration from Africa would eventually come. There is no reason Europe – especially the European Commission, the Mediterranean states and larger countries such as Germany – should have been surprised. Still, no preventive measures were taken. Instead Brussels, Berlin and Paris sent messages that encouraged the migrants.

Today, a bureaucratic paradise is being installed on global, supranational and national levels

There are plenty of other examples showing how Europe’s central authorities discriminate against member states. The reams of red tape that hinder emerging economies come to mind, such as new rules on posting workers that grossly violate the freedom of exchange of services.

Losing trust

Europe should be flourishing. The above-mentioned discriminatory measures (just a few of the striking ones among many) harm Europe. Weak political leadership results in excessive control, less freedom and [bureaucratic overreach](https://www.gisreportsonline.com/opinion-putting-europe-back-on-track,politics,2359.html).

People have increasingly begun to worry about security and prosperity. They are – unfortunately, somewhat justifiably – losing trust in democratic institutions due to weak leadership and oversized bureaucracy. As happens so often throughout history, grand initiatives and shining achievements are suffocated by their own institutions.

### Eurasia DA---AT: BRI Inevitable---2AC

#### China rise and BRI are not inevitable – it’s up to the west to stop it.

Richard Javad Heydarian, Visiting fellow at National Chengchi University, April ’20, “AT A STRATEGIC CROSSORADS: ASEAN CENTRALITY AMID SINO-AMERICAN RIVALRY IN THE INDO-PACIFIC” CONSTRAINTMENT, NOT CONTAINMENT,” https://www.brookings.edu/wp-content/uploads/2020/04/fp\_20200427\_strategic\_crossroads.pdf

None of China’s remarkable achievements, however, necessarily portend Chinese world domination, not even hegemony in Asia.14 To begin with, China suffers from acute structural vulnerabilities, including an impending demographic winter15 (i.e. that the aging population will surpass the working population within this decade) and excessively leveraged financial sector, which foretell an almost inevitable economic slowdown,16 if not worse, in the short to medium term.17 An examination of actual Chinese power — its net power of surplus resources,18 as opposed to gross resources for force projection during war — reveal a significant, if not widening, gap with more developed rivals such as the United States, which still boasts the largest pool of cutting-edge industries, Nobel laureates, high-quality human capital, and strategic natural resources.19

As structural realities catch up with China’s maturing economy, and the specter of a “middleincome trap” haunts the once-booming nation, calls for foreign policy moderation, reduced defense spending, and reconfiguration of the BRI and other ambitious overseas projects are bound to intensify. Xi would reserve the potentially disastrous rally ‘round the flag option were the domestic situation to sink to a state of political desperation, calling for unity by engaging in jingoistic and ethnocentric nationalistic discourse, as we have seen during Hong Kong protests and more recently amid the pandemic.20 More crucially, China’s geopolitical assertiveness has provoked backlash across the Indo-Pacific, most prominently in the U.S., where there is an emerging bipartisan consensus on the need to craft a robust corresponding strategy. In a sign of the changing times, even former Treasury secretary and Goldman Sachs executive Henry Paulson, a former economic advisor to China and a long-time advocate for “constructive cooperation” with Beijing,21 has warned of an “economic iron curtain.”22 Similar anxieties have influenced threat perceptions vis-à-vis China among other major players,23 including Japan, India, and the European Union, which have stepped up their military presence and strategic countermeasures in the Asia-Pacific region.24

### Eurasia DA---AT: Central Asia---2AC

#### BRI development destabilizes central asia.

Joel Wuthnow, adjunct professor in both the Eisenhower School at NDU and the Edmund A. Walsh School of Foreign Service at Georgetown University, PhD Polisci @ Columbia, MPhil @ Oxford, A.B. Princeton, proficient in mandarin, ’17, “Chinese Perspectives on the Belt and Road Initiative: Strategic Rationales, Risks, and Implications,” CHINA STRATEGIC PERSPECTIVES, Center for the Study of Chinese Military Affairs Institute for National Strategic Studies National Defense University, https://inss.ndu.edu/Portals/68/Documents/stratperspective/china/ChinaPerspectives-12.pdf

Regional Conflict

One common argument is that BRI projects are subject to the risks of operating in conflictprone areas. Lin Limin, director of CICIR’s Foreign Strategy Research Center, assesses that the SREB traverses a “geopolitical black hole,” marked by unstable regimes and rampant corruption. This has led many investors to “turn back,” and made it difficult to launch a high-speed rail network.70 Major General Wang Weixing, director of the Foreign Military Studies Department at the Academy of Military Sciences (AMS), likewise notes that “the BRI route passes through many geopolitically fragile areas, with complex historical issues, intense ethnic and religious disputes, and frequent armed conflict.”71 In another article, Wang argues that “religious violence,” in particular, can “completely throw the BRI’s construction into chaos and threaten the security of our investment projects and personnel.”72

Chinese scholars often focus on discord in specific subregions. These include the following:

■ Middle East/North Africa. Tian Wenlin, a Middle East specialist at CICIR, assesses that since the Arab Spring, the Middle East has entered its “most turbulent period since the end of the Cold War.” Specific challenges endangering infrastructure development include increasing violence between Shia and Sunni factions, especially between Iran and Saudi Arabia; the rise of separatism in areas such as southern Yemen and Libya; and the IS desire to form a state, which has split parts of Iraq and Syria.73 Other scholars note the negative consequence of the Syrian refugee crisis on Europe, which will complicate BRI projects in both regions.74 For instance, Hu Bo argues:

If West Asian and North African trends are not slowly alleviated, refugees could come swarming forward and seriously endanger eastern Europe, southern Europe, even western European countries’ governments and social stability, be a burden on economic development, and cause extremist and terrorist ideology to spread . . . and in Europe some right-wing powers still might use the confusion caused by the refugee crisis and dissatisfaction in society to change a part of the country’s domestic governance structure.75

In the maritime domain, Fu Mengzi and Lou Chunhao note that sectarian conflict in places such as Yemen and Somalia could threaten the region’s key sea lanes, such as the Strait of Hormuz, and thus the viability of the MSR.76

■ South/Central Asia. Chen Xiangyang, deputy director of CICIR’s Institute of World Politics, assesses that a reduction of U.S. forces will negatively impact the security situation in Afghanistan and “surrounding countries,” which could pose dangers for BRI projects in the region (including Pakistan).77 Fu Mengzi and Lou Chunhao write that an intensifying India-Pakistan conflict, reflected in an October 2014 border incident in Kashmir that was the deadliest since 2003, will threaten projects under both CPEC and the BCIM economic corridor.78

■ Southeast Asia. Senior Colonel Li Daguang of China’s NDU describes Southeast Asia as a “very unstable strategic direction,” involving a recent escalation of South China Sea territorial disputes and challenges from Vietnam and the Philippines, which could threaten the development of the MSR.79 Wang Weixing writes that internal instability in Thailand led to the cancellation of a China-Thailand high-speed rail plan, while internal conflict in Myanmar has led to dams and copper mine projects being halted.80

Nontraditional Security Challenges

A related issue is the impact of nontraditional security challenges on BRI projects. Perhaps the most commonly cited problem in the Chinese literature is the threat of terrorism and violent extremism. Some scholars contend that extremists might oppose the BRI on ideological grounds, since economic development strengthens existing regimes, whereas radical groups often seek to subvert them.81 Wang Yiwei also notes that development makes it harder for extremists to recruit new members and influence public opinion.82 BRI projects and workers might make attractive targets for financially motivated attacks, including kidnappings for ransom and theft of property, such as drilling machinery, oil, and communications equipment.83 Aside from direct losses, attacks could also impose indirect economic costs as firms spend more on security services and insurance premiums rise.84

Several specific groups are repeatedly identified in Chinese assessments. Those include:

■ Turkistan Islamic Party (TIP). One CICIR terrorism specialist claims that the Uighur separatist group TIP (known in China as the East Turkestan Independence Movement) has been “hiding out” in South Asia and forming “symbiotic relationships with local terrorists,” which could impact the BRI’s implementation in the region.85 Likewise, a terrorism scholar at the Northwest University of Politics and Law suggests that TIP is seeking to expand its influence into Southeast Asia, and could threaten Chinese workers involved in BRI projects, including through hostage-taking.86 Chen Xiangyang states that Uighur forces both in and outside of China launch periodic terrorist attacks, “threatening the personal safety and property of Chinese nationals.”87

■ IS. Zhang Jie, a scholar at the CASS National Institute of International Strategy, contends that foreign pressure on IS in Iraq and Syria is leading the group to expand globally and encourage “lone wolf ” attacks on targets in other countries. Based on these threats, the “risks facing Chinese personnel and investments cannot be underestimated.”88 Tian Wenlin argues that the IS desire to gain control of oil fields in the Middle East conflicts with China’s interests in oil development as part of the BRI. Another concern is that IS could influence rebel groups in Pakistani tribal regions, thus expanding the security risks facing CPEC.89

■ Pakistani Insurgents/Taliban. One CICIR South Asia specialist portrays the security situation in Baluchistan, where Gwadar and other major CPEC projects are located, as especially dangerous, recalling that Baluchi insurgents have a history of attacking infrastructure projects, including one 2006 assault that resulted in the deaths of three Chinese engineers.90 He also notes increasing activities by insurgent and Pakistani Taliban forces in Sindh Province, site of various transportation and energy projects under CPEC.91 A Central Party School researcher also assesses that insurgency poses “uncontrollable risks” to CPEC in tribal regions, blaming the Pakistani government for approving routes through these areas for political reasons.92 However, in interviews in 2017, several Chinese South Asia scholars downplayed the risks to Chinese personnel in Pakistan, pointing to a decline in the number of terrorist attacks in recent years.93

While most Chinese writings focus on terrorist threats to overseas interests, some also discuss the impact on China itself. Li Daguang notes that terrorists based in Central Asia and Afghanistan could launch new attacks in Xinjiang, which is a focal point for BRI investment within China.94 Tian Wenlin writes that IS leader Abu Bakr al-Baghdadi envisioned that Xinjiang would become part of a new Islamic caliphate, which could prompt further IS involvement in China’s northwest.95 A CASS scholar similarly predicts that Xinjiang could be threatened by Islamic militants returning from IS-held territories in the Middle East.96 More generally, a researcher at the AMS Border and Coastal Defense Research Center argues that implementing the BRI could pose new threats to China’s border security, including terrorism and international crime, and create new requirements, such as for maritime search and rescue.97 Chinese sources also discuss several other nontraditional security problems. First is piracy. Senior Colonel Liang Fang, a professor at the PLA NDU, describes piracy as a major issue along several parts of the MSR, stating that around 20 percent of Chinese ships in the Gulf of Aden have been attacked, while seven have been hijacked.98 CICIR analysts also describe an increase in the incidence of piracy in the South China Sea, where 124 incidents were reported in 2014.99 Second is drug trafficking, which Wang Weixing notes led to a 2011 plot to kill 13 Chinese sailors on the Mekong River in Myanmar.100 The third problem is environmental risks. One scholar, for instance, argues that mudslides and other natural disasters resulting from climate change could impact BRI projects “in the construction and implementation phase.”101

Despite these observations, a gap in the literature concerns the possibility that Chinese policies and practices themselves might be contributing to these risks. For instance, Wang Yiwei notes that local civil society groups, such as human rights or environmental activists, might instigate protests against BRI projects, but sees this as a result of conspiracies by “the Western world” to frustrate China’s ambitions rather than local anti-China sentiment.102 Wang and other scholars do not acknowledge that many incidents targeting overseas Chinese interests have arisen from policies such as the exclusive use of Chinese workers, poor working conditions for local employees, and collusion with corrupt local officials.103 Neither do they consider how restrictive policies on Uighur minorities might be increasing the prospects for violent incidents in Xinjiang. Lack of critical self-reflection means that China’s security community may not fully appreciate the sources of violence along BRI routes.

## Tradeoff DA

### Tradeoff DA---Thumpers---2AC

#### Tons of 5G thumpers.

Colin Demarest 22, reporter at Defense News, 4/6/2022, "Pentagon launches 5G challenge with millions up for grabs," Defense News, <https://www.defensenews.com/battlefield-tech/it-networks/5g/2022/04/06/pentagon-launches-5g-challenge-with-millions-up-for-grabs/>, RMax

WASHINGTON — The Department of Defense unveiled a multimillion-dollar 5G challenge this week that it says will promote the growth and adoption of a fifth-generation open ecosystem and related technologies.

The competition, conducted in collaboration with the National Telecommunications and Information Administration, focuses on open interfaces, swappable and compatible parts, and the development of a diverse, multi-vendor community.

Participants who submit hardware or software solutions for 5G network subsystems that meet exacting criteria will be eligible for awards of up to $3 million, the Pentagon said in an April 6 announcement.

Amanda Toman, DoD’s acting principal director of 5G and similar capabilities, in a statement said the department “is committed to supporting innovation efforts that accelerate the domestic development of 5G and future-G technologies. 5G is too critical a technology sector to relinquish to countries whose products and technologies are not aligned with our standards of privacy and security.”

Fifth-generation wireless technology boasts boosted bandwidth, reduced latency and much faster speeds compared to its predecessors. Those factors make 5G — and what comes after — critical to the Defense Department, which has increasingly emphasized the importance of unrestricted and speedy information sharing.

A closed-off, siloed wireless industry has driven up costs, hamstrung innovation and dulled competition, according to the Pentagon, and the new challenge aims to change that. The National Telecommunications and Information Administration in a video published April 6 said the Defense Department, international allies, network operators and consumers will benefit.

“We will continue our support of all necessary efforts to unleash innovation while developing secure 5G supply chains,” Toman said.

The Defense Department in 2020 said it would invest $600 million in 5G testbeds at five military installations across the U.S. Additional investments were made in 2021.

More recently, the Defense Department announced the establishment of a 5G and Future-G Cross Functional Team that will work to ensure U.S. forces can operate anywhere, including in environments where networks are contested and communication is difficult.

“Today’s operational requirements call for the acceleration of 5G technology with at-scale prototyping and experimentation,” Toman said in a March 9 statement. “The 5G and Future Generation CFT will play a critical role in advancing the department’s 5G and future generation capabilities.”

Applications for the challenge are open through May 5.

### Tradeoff DA---Thumpers---1AR

#### Test beds and FY2023 thump.

Colin Demarest 22, reporter at Defense News, 4/19/2022, "5G deemed a ‘great enabler’ for US Navy," C4ISRNet, <https://www.c4isrnet.com/battlefield-tech/it-networks/5g/2022/04/19/5g-deemed-a-great-enabler-for-us-navy/>, RMax

The [Department of Defense](https://www.c4isrnet.com/artificial-intelligence/2022/04/15/us-and-india-launch-talks-about-military-ai/) has selected a dozen military installations as test beds for 5G, including sites in California, Georgia and Virginia. This month, the department unveiled a multimillion-dollar challenge to accelerate the growth and adoption of a fifth-generation open ecosystem.

AT&T Inc. this year claimed initial success in setting up a 5G network experiment that could realize smart warehouses for the Navy, [Defense News reported](https://www.defensenews.com/smr/5g/2022/02/01/att-sees-progress-in-navys-5g-smart-warehouse-experiment/). The service believes smart warehouses could boost the efficiency and fidelity of its logistics.

“When we first started experimenting and piloting in 5G,” Galbraith said Tuesday, “we looked at what our priorities were.”

The Defense Department received nearly $338 million for 5G and microelectronics in fiscal year 2022. It requested $250 million for fiscal year 2023, [budget documents](https://www.c4isrnet.com/cyber/2022/03/28/pentagon-seeks-112-billion-for-cyber-in-fy23-budget-request/) show.

#### 5G to NextG thumps.

Partyard 22 – Partyard Military Division, worldwide supplier of OEM systems and aftermarket air, sea, and land spares and maintenance, 3/8/2022, "​​Why the World’s Militaries Are Embracing 5G," <https://partyardmilitary.com/2022/03/08/why-the-worlds-militaries-are-embracing-5g/>, RMax

No wonder, then, that the U.S. Department of Defense, through an initiative called 5G to NextG, and various complementary investments from individual armed services, has committed upwards of US $2 billion to advance commercial 5G research and to perform tests and experiments to adapt the results for military purposes.

#### Military 5G funding is inevitable.

Greg Nichols 20, journalist and contributor to ZDNet, 10/21/2020, "Digital fortress: 5G is a weapon in national defense," ZDNet, <https://www.zdnet.com/article/digital-fortress-5g-a-weapon-in-national-defense/>, RMax

Amateurs talk strategy, professionals talk logistics. In the 2020s, that old chestnut should probably be updated: "Professionals talk about the network."

And boy are they talking. The U.S. government will be one of the [biggest spenders](https://tbri.com/special-reports/private-5g-networks-market-will-see-strong-growth-as-a-broad-range-of-industries-and-governments-adopt-the-technology/) on private 5G infrastructure, and the Department of Defense leads the pack. DoD's growing network demands include connecting in-field technology as well as supporting day-to-day base operations and force training. DoD's need for increased connectivity is driving greater investment in 4G LTE, but that's only laying the foundation for a massive shift to 5G.

It turns out that shift is already underway. According to Lt Col Brandon Newell, Director, SoCal Tech Bridge, NavalX, since July of this year the 5G Living Lab aboard MCAS Miramar, a partnership with Verizon, has been active, representing the first 5G Ultra Wideband mmWave deployment on a military installation in the nation.

"Our intent is to embrace 5G-enabled tech that is being used to advance commercial industries as a weapon in the Defense Market," says Lt Col Newell. "We are embarking to explore base resilience through energy management and communications, security through what we call 'the digital fortress,' and mobility across modalities such as autonomous vehicles and unmanned aerial systems."

In other words, 5G will serve as the undergirding for a new generation of warfighting.

"More so than with other technologies in the past, we're seeing that the Department of Defense (DoD) and military leaders realize how important 5G is for their departments and are eager to adopt it," says Nick Nilan, Director of Product Development, Public Sector for Verizon, who helped me understand the scope of adoption. "Military leaders across the country are improving their infrastructure so they are ready to take advantage of 5G. Widespread cloud adoption over the last few years has also driven an increased demand for better connectivity. In order to access information in the cloud anywhere, anytime, you need better connectivity – you need 5G."

#### Current DOD 5G thumps.

Jon Harper 21, (analyst and writer who the Pentagon and military technology 12-10-2021, "‘A lot of work’ still required to enable 5G integration for U.S. military," FedScoop, <https://www.fedscoop.com/5g-interoperability-neal-ziring-nsa/> )/billy

The Department of Defense has ambitious plans to leverage 5G communications technology for a wide variety of use cases to include back-office functions, logistics, training and warfighting. However, a great deal of work remains to be done by government and industry to ensure those systems and networks will be secure and interoperable when they are deployed, according to a top National Security Agency official.

The Pentagon has a number of 5G pilot projects underway. In the future, observers can expect a “full wave” of these next-generation capabilities to be fielded, said Neal Ziring, technical director of the cybersecurity directorate at NSA.

“We’re looking at our biggest customers, the [military] services, and saying, ‘Wow, they’re rushing headlong towards 5G,’” Ziring said Wednesday during a luncheon hosted by AFCEA.

NSA wants to help. To that end, a number of steps need to be taken to meet the security, interoperability and deployability requirements for defense applications, he noted.

One is ensuring the right standards are in place. A number of organizations are involved in setting those standards.

“Those standards bodies define how the 5G gear works together. So, NSA and other parts of the DOD and parts of the industrial base who are represented here today, especially the telecommunications carriers, are active in that environment trying to make sure that those standards have security baked into them so that all the equipment we buy from whatever vendor … have the security in it that we need, and that we can turn it on or request that our industry service providers make full use of it in providing service to defense,” Ziring said.

Another key component of the next-gen communications technology will be a concept known as network slicing, which will enable service providers to set up independent logical networks across the same 5G infrastructure.

“They sort of have it a little bit in 4G, but it’s a big feature in 5G,” Ziring said. “We think that’s going to be really important for pretty much all the defense use cases.”

Managers can designate specific network “slices” for certain users or certain devices, and then provide levels of security protection, isolation or access to only the authorized members of that slice, he explained.

### Tradeoff DA---Normal Means---2AC

#### Normal means would use new authorities for implementation

Leleux et al ’21 [Darrin, Deputy Director of the Electromagnetic Spectrum Operations Cross-Functional Team earned his Master of Science in Computer Engineering from the University of Houston at Clear Lake in 1998, and a PhD in Electrical Engineering from Rice University in 2002, Winter 2021, “Fifth Generation Wireless Development in Great Power Competition,” Cyber Defense Review, <https://cyberdefensereview.army.mil/Portals/6/Documents/2021_winter_cdr/02_CDR_Winter_2021_Leleux.pdf?ver=X83q7TOOVMvhrIJHxhBw_A%3D%3D>, St. Mark’s, AM]

USG systems must be able to determine that an attack, malicious event, or exploitation is in progress to take timely actions to ensure system resilience. To identify early warning of an anomaly or attack, US entities must understand their standard day-to-day environment, sense that something is out of the ordinary, and determine what is happening across the digital domain.[37] Additionally, as DoD implements equipment that can leverage the 5G wireless infrastructure, military communications operators need to be trained and have the right tools to detect outside influence. Once an attack is identified, the more difficult task is attributing the activity to a malicious actor and then identifying the attack vector. To accomplish this, DoD should improve training programs for its cyber warriors and develop tools that can detect anomalies and potentially take the first steps in countering cyber-attacks. To help identify attack vectors and determine where an attack came from, new authorities or adjustment to current authorities may be required, especially if autonomous actions are incorporated into these systems.

### Tradeoff DA---AT: Cooperation---2AC

#### DoS 5G diplomacy with NATO now thumps.

Marius Ghincea 21, Ph.D. Researcher at the European University Institute, 04-2021, “WHO SUMMONS THE DRAGON?”, <https://eastern-focus.eu/wp-content/uploads/2021/06/GlobalFocus_China%E2%80%99s-demand-driven-in-uence-in-CEE-and-WB.pdf>, global focus //billy

Calling upon the so-called Prague 5G Security Proposals, in 2020 the US government launched the bi-partisan ‘Clean Network’ initiative aimed at addressing the threats to data privacy, security and human rights from authoritarian malign actors. Directly targeting the Chinese telecommunication giants like Huawei and ZTE – accused of being ‘untrusted vendors’ required to observe the directives of the Chinese Communist Party – the US’s 5G diplomacy has actively engaged in ensuring support from countries across the world, especially from its NATO and EU allies in Europe. As a result, most European countries have signed bilateral memoranda of understanding with the United States agreeing not to pursue equipment from such ‘untrusted vendors’ in the development of their national 5G infrastructures.

### DSCA---No Link---2AC

#### No link---Ukraine SC comes from a separate pool.

Lorin Venable 7/8, Assistant Inspector General for Audit Financial Management and Reporting, “Management Advisory: The DoD’s Use of Ukraine Supplemental Appropriations Act, 2022 Funds,” <https://media.defense.gov/2022/Jul/12/2003033575/-1/-1/1/DODIG-2022-112.PDF>, RMax

We determined that as of June 2, 2022, the Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, DoD, (OUSD[C]/CFO) has implemented procedures for DoD Components to follow in reporting through Advancing Analytics (Advana) the execution of the $6.5 billion in funds appropriated to the DoD to provide assistance to Ukraine.1 OUSD(C)/CFO personal implemented processes to help ensure DoD Components are reporting, through their respective accounting systems, the transactions supporting the assistance the DoD is providing to Ukraine. However, the DoD’s use of systems that are not able to directly feed into Advana could limit the transparency of the execution of the Ukraine supplemental funds.

Background

The President enacted the Ukraine Supplemental Appropriations Act, 2022 (the Act) on March 15, 2022 as part of the Consolidated Appropriations Act, 2022.2 Congress designates each amount provided by the Act as being for an emergency requirement.3 The Act provided the DoD with $6.528 billion in funds for assistance to Ukraine, specifically:

• $3.028 billion directly appropriated for U.S. European Command operations mission support, the deployment of personnel to the region, and intelligence support; and

• $3.500 billion of reprogramming funds to replace the DoD’s stocks, and to reimburse the DoD for defense services, education, and training provided to Ukraine.

The Act requires that the $3.5 billion remain available for transfer under the appropriation “Operation and Maintenance, Defense‑Wide.” These funds may only be transferred to accounts under the heading “Operation and Maintenance” and “Procurement” for the replacement of defense articles from DoD stocks and reimbursement for services. Furthermore, the Act requires the Secretary of Defense to notify the congressional defense committees of the details of transfers at least 30 days before any transfer, and the funds transferred must be used for the same purposes and same period as the appropriations to which the funds are transferred.

#### They got a lot of money.

Lorin Venable 7/8, Assistant Inspector General for Audit Financial Management and Reporting, “Management Advisory: The DoD’s Use of Ukraine Supplemental Appropriations Act, 2022 Funds,” <https://media.defense.gov/2022/Jul/12/2003033575/-1/-1/1/DODIG-2022-112.PDF>, RMax

The DoD received $6.5 billion in funding under the Ukraine Supplemental Appropriations Act:

• $3.5 billion for reprogramming to replenish DoD Stocks and reimburse DoD services

• $2.1 billion for Operations and Maintenance

• $409.0 million for Defense Working Capital Funds

• $227.1 million for Procurement

• $195.5 million for Military Personnel

• $130.3 million for Research, Development, Test, and Evaluation

## Politics

### Politics DA---No Link---2AC

#### Congress supports 5G development and already directed the DOD to deploy 5G.

John R. Hoehn and Kelly M. Sayler 20 (analysts in Military Capabilities and Advanced Technology, 11-8-20, “National Security Implications of Fifth Generation (5G) Mobile Technologies”, congressional research service, <https://nsarchive.gwu.edu/sites/default/files/documents/r1xccm-260rw/20201008%20IF11251.pdf>) /billy

National Security Concerns

According to a DIB assessment, China is the current leader in sub-6 technologies and is likely to deploy the world’s first 5G wide-area network. Chinese companies, which often receive government subsidies (e.g., subsidized land for facilities, R&D grants), are therefore well-positioned as global 5G suppliers. Huawei has signed contracts for the construction of 5G infrastructure in around 30 countries, including Iceland, Turkey, and the United Kingdom. Some experts are concerned that vulnerabilities in Chinese equipment could be used to conduct cyberattacks or military/industrial espionage. These experts claim vulnerabilities were introduced through the poor business practices of many Chinese companies. However, they note that vulnerabilities could also be intentionally introduced for malicious purposes. China’s National Intelligence Law, enacted in June 2017, declares that “any organization and citizen shall, in accordance with the law, support, provide assistance, and cooperate in national intelligence work, and guard the secrecy of any national intelligence work that they are aware of.” Some analysts interpret this law as requiring Chinese companies to cooperate with intelligence services, including compelling installation of backdoors to provide private data to the government. Other analysts argue that the risks posed by Chinese telecommunications equipment vary depending on the equipment’s location within the cellular network architecture. Most cellular networks are broken into two groups: the core network, which provides the gateway to the internet and ensures devices meet the provider’s standards, and the radio access network, composed of the cellular towers that broadcast and receive radio signals (see Figure 2). These analysts state that, while the risks posed by Chinese core networks are significant, the risks posed by Chinese radio access networks could be managed. Other analysts have argued that having any Chinese equipment in the network could pose potential security concerns. Such concerns have prompted some analysts to argue that the United States should limit intelligence sharing with any country operating Chinese-supplied 5G equipment. In response to these national security concerns, Congress passed the Secure 5G and Beyond Act of 2020 (P.L. 116- 129), requiring the President to develop a strategy to protect 5G systems and infrastructure in the United States and assist allies and partners in their own protection efforts. The Administration released its 5G strategy in March 2020. Similarly, in Section 254 of the FY2020 National Defense Authorization Act (P.L. 116-92), Congress directed DOD to develop a strategy to harness 5G “to enhance military capabilities, maintain a technological advantage on the battlefield, and accelerate the deployment of new commercial products and services enabled by 5G networks throughout the Department of Defense.” DOD released an unclassified version of this strategy in May 2020.

Implications for Military Operations

5G technologies could have a number of potential military applications, particularly for autonomous vehicles, C2, logistics, maintenance, augmented and virtual reality, and ISR systems—all of which would benefit from improved data rates and lower latency (time delay). Autonomous military vehicles, like their commercial counterparts, could potentially circumvent on-board data processing limitations by storing large databases (e.g., maps) in the cloud. Safe vehicle operations would require 5G’s high data rates and low latency to download off-board information and synthesize it with on-board sensor data. Likewise, 5G could be used to transfer sensor data between operators and uninhabited vehicles and to network vehicles, potentially enabling new military concepts of operations, such as swarming (i.e., cooperative behavior in which vehicles autonomously coordinate to achieve a task). 5G technologies could also be incorporated into ISR systems, which increasingly demand high-bandwidths to process, exploit, and disseminate information from a growing number of battlespace sensors. This could provide commanders with timely access to actionable intelligence data, in turn improving operational decisionmaking. Similarly, 5G could reduce latency in other data-intensive activities, such as logistics and maintenance, and could additionally enable augmented or virtual reality environments that could enhance training. Finally, command and control systems could benefit from the high speed, low latency capability of 5G. For example, the U.S. military currently uses satellite communications for most of its long-distance communications. However, satellites on orbit can significantly increase latency due to the amount of distance a signal needs to travel, causing delays in the execution of military operations. Although DOD is in the initial stages of testing and experimentation for 5G applications, it has selected 12 military installations as test beds: Marine Corps Logistics Base Albany, GA, and Naval Base San Diego, CA (“smart warehouses”); Hill Air Force Base, UT (“spectrum sharing between 5G and airborne radar”); Joint Base LewisMcChord, WA (“augmented and virtual reality”); Nellis Air Force Base, NV (“survivable command and control and network enhancement”); Naval Base Norfolk, VA (“shipwide and pier connectivity”); Joint Base Pearl HarborHickam, HI (“enhancing aircraft mission readiness”); Joint Base San Antonio, TX (“augmented reality support of maintenance and training” and “evaluating DOD's 5G core security experimentation network”); Tinker Air Force Base, OK (“spectrum sharing between military communications and 5G”); and Camp Pendleton, CA; Ft. Hood, TX; and Ft. Irwin National Training Center, CA (“connectivity for forward operating bases and tactical operations centers”). On September 18, 2020, DOD issued a request for information to better understand dynamic spectrum sharing for 5G technologies. DOD requested $1.5 billion for 5G and microelectronics in FY2021.